An Evolution Roadmap for Community Cyber Security Information Sharing Maturity Model

Wanying Zhao
The University of Texas at San Antonio
kallenzwy@gmail.com

Gregory White
The University of Texas at San Antonio
Greg.White@cs.utsa.edu

Abstract

Cyber security has become one of the most important challenges, which is especially true for communities. A community generally consists of all of the entities within a geographical region, including both public and private infrastructures. Cyber attacks and other cyber threats can result in disruption and destruction of critical services and cause potentially devastating impacts in a community.

An effective information collection, sharing and incident collaboration and coordination process is needed in communities to detect potential risks, prevent cyber attacks at an early stage, and facilitate incident response and preparedness activities. In this paper, an expanded collaborative information sharing framework that aims to improve community cyber security is presented. An Information Sharing Maturity Model is developed as a roadmap with evolutionary procedures and incremental steps for community organizations to advance in information sharing maturity.

1. Introduction

Today, as more daily functions are digitized and the reliance of communities on critical cyber infrastructures keep growing, cyber security has become one of the most important challenges. Generally, a community consists of all of the entities within a geographical region, including both public and private infrastructures, such as finance, utilities (*e.g.* energy and water), health care and other important sectors. Cyber attacks and other cyber threats can result in disruption and destruction of critical services and cause potentially devastating impacts in a community.

Many efforts at national and state levels were developed to address cyber security awareness and cyber incident response and coordination. At a national level, U.S. President Obama's initiative to improve the nation's cyber security posture, the Cybersecurity National Action Plan (CNAP), calls for near-term actions and a long-term strategy to enhance cyber security awareness and protections, protect privacy, maintain public safety as well as economic and national security. The National Cyber Incident Response Plan [1] was developed according to the principles outlined in the National Response Framework. It describes how the nation responds to significant cyber incidents. At a state level, the Multi-State Information Sharing and Analysis Center (MS-ISAC) was established and serves to improve the overall cyber security posture of state, local, territorial and tribal governments. However, in most communities there is no collaboration process or developed framework for effective information collecting, sharing and incident collaboration and coordination specifically designed for community cyber security.

Several information sharing platforms currently in use or under development are introduced in the work [2], [3] and [4]. Related efforts include projects such as Collective Intelligence Framework (CIF) [5], Cyber security Information Exchange Framework (CYBEX)[6], and Cyber Security Data Exchange and Collaboration (CDXI) [7]. Some of these research projects and information sharing frameworks are still under development. Although these works present high relevance to this research and provide a lot of insights, they are not necessarily suitable for information sharing in a community. Most of these works adopted a centralized approach for information sharing without addressing the lack of coordination within a community or among the sectors in a community. Collaboration and coordination is needed among the entities within a community. The approach in this paper is specifically designed for the community information sharing environment.

In recent years, the Community Cyber Security Maturity Model (CCSMM) [8] developed by the Center for Infrastructure Assurance and Security (CIAS) at

URI: http://hdl.handle.net/10125/41443
ISBN: 978-0-9981331-0-2

The University of Texas at San Antonio was proposed to help communities establish viable and sustainable cyber security programs. To address information sharing, one of the most important aspects of CCSMM, a collaborative information sharing framework specifically designed for a community was developed to facilitate collaborative information sharing among the organizations and entities in the community itself [9]. Information sharing requirements and a formal policy model for this framework were presented [10].

In this paper, we present an extended collaborative information sharing framework by incorporating interaction with other internal and external information sharing agencies (such as Fusion Centers and Emergency Operation Centers) for a community. Currently, in most communities, organizations do not share or only share minimal informal information with other entities. It will take incremental steps for a community to establish such a framework. It is important to provide a roadmap for communities to evolve in maturity levels and establish this framework gradually. In this paper, we present the Information Sharing Maturity Model and provide the roadmap and appropriate evolution process details for a community to advance in the five maturity levels. This paper presents this framework as a conceptual design, the implementation detail will vary depending on fulfillment in specific communities.

The rest of the paper is organized as follows. Section 2 presents our extended collaborative information sharing framework for community cyber security. Section 3 discusses the Information Sharing Maturity Model in the community and the key aspects of the model. Section 4 presents a roadmap and evolution process details for a community to advance in information sharing maturity from level 1 through level 5 with specific information sharing events at each level as examples. Section 5 discusses future work and section 6 concludes the paper.

2. Collaborative information sharing framework in a community

Previously based on the group-based information sharing model, a collaborative information sharing framework [10] specifically for community cyber security was proposed, in which different types of groups were defined and various inter-group relationships were introduced. The framework was designed to facilitate information sharing but at the same time protect information deemed sensitive by its owners within groups.

We extended the framework by incorporating interaction with other internal and external information sharing agencies for a community. In our extended framework, shown in Figure 1, ***Sector Groups*** represent the major sectors in communities. These include energy, water, finance, healthcare, emergency services, telecommunications, transportation, *etc.* ***Non-Sector Organizations*** provide information from academia, other industry entities, and even individual citizens. The ***Super Group*** is responsible for obtaining information from internal and external sources, performing intelligence information analysis, and coordinating information sharing and incident management among different Sector Groups. The ***Collaboration Group*** provides an established, long-term collaboration mechanism for information sharing among different sectors to share information applicable to all members in the community (such as community-wide alerts or warnings). It also provides the foundation for sectors to correlate incident details to determine when to establish a group for specific incidents. An ***Incident Group*** supports incident-specific information sharing when incidents occur in the community. A new Incident Group is created when a threat to the community is identified related to an incident or a specific type of incidents, related community members will join the Incident Group to share further details about the incident(s).

Our extended framework also introduces two additional important roles in providing information gathering and incident handling for general incidents (not necessarily cyber incidents) to support the country's homeland security efforts: ***Fusion Centers*** [11], which share information across all levels of government to support homeland security partners in preventing, protecting against, and responding to crime and terrorism; and ***Emergency Operation Centers (EOC)***, which primarily provide information and support to incident management and response/recovery coordination activities at all levels of government.

The groups in this framework aim at sharing cyber threat/incident related information and cyber incident response. Together with a fusion center and EOC, they serve distinct but complementary roles in supporting the community cyber security efforts. Interaction and collaboration among cyber information sharing entities, fusion centers, and EOCs will enable them all to carry out their own mission more effectively.

In an ideal scenario displayed in Figure 1, a dedicated fusion center resides in the community. The Super Group representatives need to collaborate with the fusion center for enhancing information analysis and local fusion. And they need to share cyber threat related information they collected, aggregated and analyzed (within a cyber context) with the fusion center. The fusion center is responsible for combining and

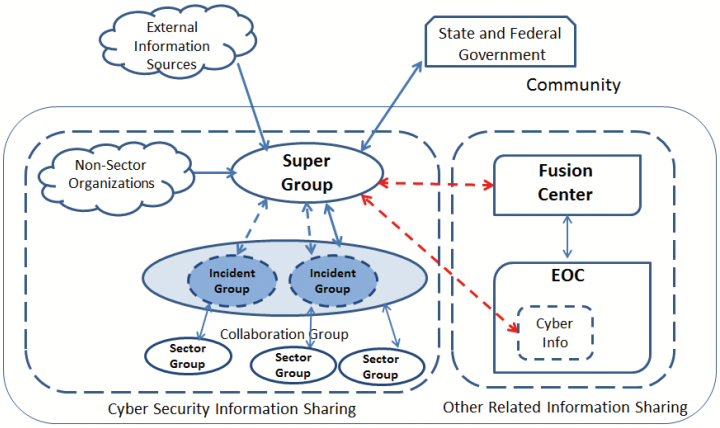

Figure 1. The Collaborative Information Sharing Framework in a Community

analyzing the threat intelligence including both cyber and physical evidence from all available sources. It needs to send the fused cyber threat intelligence to the Super Group representatives, then the Super Group will disseminate appropriate threat information to the community. If there is no dedicated fusion center in the community, the Super Group representative needs to collaborate with external organizations such as the state level fusion center and the state Chief Information Security Officer (CISO) and provide comparable local fusion service.

The Super Group representatives also need to collaborate with the EOC in the community by sharing cyber incident related information. The EOC is responsible for providing appropriate incident response and coordination to the Super Group representative who can then share the incident response to related Incident Groups. This requires that the EOC be able to handle cyber security incidents. However, currently most EOCs do not have any or have only minimal cyber security capability. As the community becomes mature from a cyber security standpoint, some cyber security experts and advisors from the Super Group could participate in assisting the EOC. Later on, the EOC could form their own cyber security unit as they grow their the capability for handling cyber incidents just as they have expertise for other potential incidents such as fire or weather related incidents.

3. Key aspects of information sharing maturity model

As a result of the need to better define methods to determine the current status of a community in its cyber preparedness, and in order to provide a roadmap for communities to follow in their preparation efforts, the Community Cyber Security Maturity Model (CCSMM) [8] was established to address the needs of states and communities in developing a viable and sustainable cyber security program. There are five maturity levels for the organization, community, and state respectively. At each level, there are several main aspects. As one of the most important aspects, the information sharing aspect for the community dimension can be pulled out as an Information Sharing Maturity Model of the CCSMM. We depict our Information Sharing Maturity Model as presented in Figure 2.

There are mainly three key aspects of maturity in the Information Sharing Maturity Model: technology maturity, policy maturity and management maturity. Figure 2 outlines the three key aspects through the five levels of the Information Sharing Maturity Model. For each of the three maturity aspects, a few related major issues are listed. The maturity key aspects and related issues will be discussed in detail in this section. The specific maturity measurement at each level and how these maturity key aspects evolve from level 1 through level 5 will be discussed in the next section.

3.1. Technology maturity

Technology maturity mainly focuses on the maturity of the technology needed in information sharing, including the communication methods, information exchanging formats and information analysis technology to process the shared information.

Communication: The methodologies, techniques, and tools for communication among information sharing participants vary at the different maturity levels. At the initial level which begins with no community information sharing, no group is formed. Information sharing informally occurs between pairs of entities.

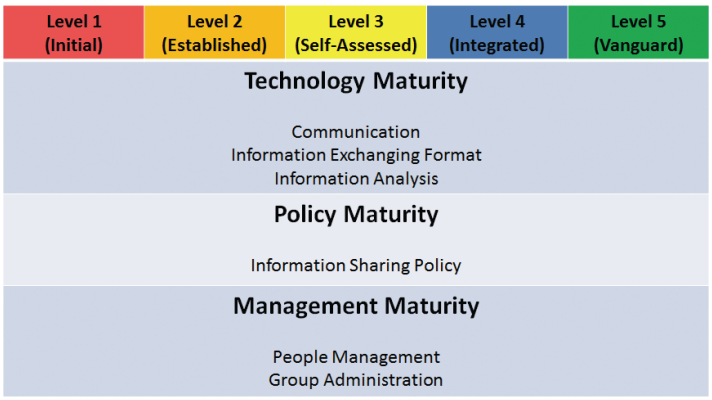

Figure 2. Key Aspects of Information Sharing Maturity Model in the Community

The communication method is mainly via phone call, email, or personal contact. As the information sharing maturity level advances and as different types of groups are formed, appropriate group communication methods should be established. Communication tools such as mailing lists, instant messaging, shared data repositories, message boards, and real-time web conferencing could be utilized for specific needs of different communities.

Information exchanging format: At Level 1 and Level 2 with informal information sharing, structured information and standardized information exchanging format may not be necessarily needed. As more tools assisting automated information sharing (*e.g.* Automated Indicator Sharing provided by DHS) and information analysis become available at the higher maturity levels, the need for structured cyber threat information representation increases. In recent years, several standards have been developed for exchanging organized, structured, and described cyber threat related information, such as OpenIOC [12], The Incident Object Description Exchange Format (IODEF) [13], The Structured Threat Information eXpression (STIX) [14], The Trusted Automated eXchange of Indicator Information (TAXII)[15].

Information analysis: At Level 1, there is no information analysis or only local, ad-hoc information analysis. At level 2, the information sharing participants manually perform informal information analysis, provided that they are capable of it. As the maturity level advances, there should be tools available for automated data aggregation, correlation and formal analysis. At higher maturity levels (4 and 5) information analysis also includes data fusion which combines technical intelligence and human intelligence, cyber evidence and physical evidence.

3.2. Policy maturity

Policy maturity evaluates the maturity of information sharing policies. At the initial level, there is no information sharing policy defined. As the community maturity level advances, information sharing policies should be defined and implemented in the different types of groups according to their function. The Information sharing policy should be a document specifying purpose, scope, what information needs to be collected, when information needs to be collected, how the collected information will be used, security and privacy policy, data governance policy *etc.*

3.3. Management maturity

Management maturity evaluates the maturity level of management activities including people management and group administration.

People management: People management basically includes the evaluation of availability and qualification of personnel for information collection, aggregation, analysis and incident coordination, selection of appropriate group representatives in Sector Groups and cyber threat analysts in the Collaboration Group. It also includes the training and exercise associated with the appointed tasks.

Group administration: In a Sector Group, group administration includes admitting appropriate individuals to become a group member according to predefined policies, maintaining and updating information policies in the group, organizing group meetings for discussion when changes of policies or procedures to be made to the group, and other group activities. In the Collaboration Group, group administration also includes creating or deleting an Incident Group and managing all Incident Groups.

4. Evolution process of information sharing maturity model

Currently, in most communities, organizations do not share or only share minimal informal information with other entities. Advancing towards higher maturity levels, a community could gain more comprehensive cyber intelligence from various sources to detect potential risks and prevent cyber attacks at an early stage, share information and coordinate incident response as well as preparedness activities more effectively.

In reality the mechanisms for collaborative information sharing cannot be established in an instant. It will take a series of incremental steps for a community to evolve from Level 1 to Level 5 of the Information Sharing Maturity Model. During the evolution process they gradually establish groups, specify policies and adapt appropriate information exchanging methods. It is important to provide a roadmap with appropriate evolution process details for a community to advance in information sharing maturity levels. This section will specify the requirements of policy maturity, technology maturity and people maturity at each level and provide a roadmap of evolution process for a community to advance towards higher maturity levels.

To establish a formal collaborative information sharing framework as described in Section 2 and effectively use information shared to enforce community cyber security, every community should at least target Level 3. Whether a community needs to reach Level 4 or 5 depends on the scale, the population, potential threats to the community, and the cyber security capability of the community. Communities also need to balance the cost of establishing mechanism, professional personnel and techniques and the benefit of gaining better protection from cyber incidents as the they advance to higher maturity levels.

4.1. Level 1 (Initial)

4.1.1. Overview of Level 1. Information sharing at this level is among individuals within organizations and between individuals in different organizations in the community. There is no or minimal security related information of individual organizations being shared at this level. The minimal information include notice and inquiry about suspicious or unusual activities, warnings or alert messages. This level is the start of the process and assumes no established information sharing processes.

4.1.2. Maturity at Level 1. There is no or minimal informal information sharing between entities within the community and no or minimal information is shared with appropriate organizations or agencies. Any information sharing is ad-hoc.

- Technology Maturity: Individuals use Email, phone calls or other personal contact to communicate between each another. The information exchanging format is informal and not structured. Information analysis is ad-hoc and depends on the capability of individuals.
- Policy Maturity: There is no information sharing policy defined.
- Management Maturity: There is no special personnel or organization formed for information sharing.

Examples of information sharing for a security-related event at Level 1 are given below:

Event 4.1: A staff member in organization A detects some port scanning and does not report it to anyone.

Event 4.2: Network administrator A in Bank X notices some suspicious network traffic on a handful of ports. He calls administrator B, who he knows, by phone and asks if administrator B has noticed similar suspicious network activities in Bank Y. B then performs network monitoring and tracing and finds that there has been increased network traffic coming from a common IP address A provided. Both of them update firewall packet filter rules to limit traffic from the IP address.

4.1.3. Efforts to reach Level 2. There are several steps to accomplish to reach the next level.

Prior to establishment of a Sector Group, organizations in that sector should become prepared for cyber security related information sharing, this includes:

- Establish the personnel responsible for cyber security related management, the staffs may include the Computer Security Incident Response Team Manager, network administrators, system administrators, and other cyber security related employees.
- Conduct preliminary education of the necessity and importance of cyber security awareness to all personnel and information sharing for those responsible to address cyber incidents.

As the maturity of the community progresses, it will need to start to expand information sharing to a group of organizations. The first step is forming a Sector Group and establishing information sharing in the Sector Group. This can be accomplished by:

- Organization security leaders from the same sector get together and form a Sector Group, with

discussion of which staff members would participate in the information sharing, what information is to be shared and what method will be used for information sharing
- In the scope of each Sector Group, specify informal information sharing security policies as an initial agreement on what cyber threat information will be shared with other participants in the Sector Group, how the shared information should be processed and the mechanism admitting new members to the group.
- Each sector establishes a mechanism to select appropriate Sector Group representative(s) responsible for information aggregation, incident reporting, initial information analysis, and define a memorandum of agreement regarding the details for all members to sign.
- Each sector selects a group administrator to perform group administration and maintain and update information sharing policies. (The group administrator in a Sector Group can be a group representative mentioned above, or another group member.)
- Develop an appropriate and convenient group communication service that suits the sector members. (*e.g.* mailing lists as the primary communication method, web conferencing as the secondary communication method.)

Besides sectors, the following effort should be done for the awareness of local government and external information sharing outside the community.

- Establish a Mayor's cyber security advisory group to advise the mayor on cyber security events.
- Encourage establishment of information sharing and professional networking organizations such as ISSA and InfraGard if the community doesn't already have chapters of them.

A critical element to the success of any cyber security program within both an organization or a community is the presence of a "champion" for security. The community will need an individual who can help encourage organizations and sectors to select their representatives and to begin to organize within their sector.

4.2. Level 2 (Established)

4.2.1. Overview of Level 2. Information sharing at this level is among Sector Group members within the same sector, these Sector Group members are from the organizations forming that sector. Certain amount of information is shared with external entities (a sector-specific ISAC or US-CERT) informally. Information shared at this level includes but is not limited to: threat indicators, warning, alert or incident information, details about specific cyber incidents, and mitigation strategies.

4.2.2. Maturity at Level 2. At this level, information sharing and collaboration among entities within each Sector Group are established. Data aggregation and initial information analysis are conducted by representatives in each Sector Group. The mayor's cyber security advisory group and/or other security professional agencies are established and engaged in informal communication.

- Technology Maturity: Organizations use basic group communication tools for information exchanging in each Sector Group. The information exchanging format is not standardized. Providing an informal structured template such as a form covering crucial information is suggested. Initial, local ad-hoc information analysis and aggregation is performed in each Sector Group manually or with assistance of tools.
- Policy Maturity: In each Sector Group, informal information sharing policies within that sector are defined.
- Management Maturity: In each Sector Group, a mechanism to select appropriate representatives for the Sector Group is established, group administration is performed by a group administrator.

An example of information sharing for a security-related event at Level 2 is given below:

Event 4.3: An alert "Penetration occurred on March 1, 2012, the attack is from IP address 123.123.123.123. The attack is aimed at port 4567 used by application X." from organization A was sent via a group broadcasting message to all other members in the same sector. Later a staff member in organization B sent a new group message stating that a lot of traffic from the same IP address aimed at the same port was noticed, followed by three other members reporting the same traffic. The Sector Group representative then determined potential mitigation strategy and response actions and initiated a group session to discuss it.

4.2.3. Efforts to reach Level 3. There are several tasks to accomplish for a community to reach the next information sharing maturity level.

The following should take place for the Super Group:

- A formal Super Group should be formed and staffed by security experts in the community. (This group could evolve from the Mayor's cyber security advisory group).

- The Super Group establishes connections to import information from Non-Sector Organizations and external sources (*e.g.* via data feeds) and establishes informal communication with external entities such as the state and federal government.

The following should be accomplished for the Collaboration Group and Incident Group establishment and maintenance:

- Form a formal Collaboration Group. The representatives from all Sector Groups and the Super Group get together and decide on issues such as what information to be shared based at what frequency, what communication and information analysis tools should be used, what the administration mechanism of the Collaboration Group should be.
- Specify formal information sharing policies for what sorts of cyber threat information will be shared with other participants in the Collaboration Group and Incident Groups and how the shared information should be processed based on agreement of trust and privacy concerns.
- Establish a mechanism to authorize appropriate Super Group members and Sector Group representatives to join the Collaboration Group.
- Assign appropriate representatives as the administrators of the Collaboration Group.
- Develop appropriate and convenient group communication tools that suit the group members.
- Select an information exchanging standard to formalize the shared information.
- Appoint selective Super Group representatives to the Collaboration Group as cyber threat analysts responsible for information analysis and incident coordination of the community.
- Develop the formal information analysis methodology with the assistance of available tools and techniques.
- Define the metrics and criteria for measuring the threat alert level for the whole community and when a threshold is reached for identifying a potential threat to the community.
- Develop a mechanism to maintain an Incident Group, including the creation of the Incident Group when a potential threat is identified to the community, authorizing related members to join the Incident Group, management of the incident, and the deletion of the Incident Group when the incident is resolved. Define the administration and management duties of the Incident Group and assign the tasks to the administrators and cyber threat analysts.

4.3. Level 3 (Self-Assessed)

4.3.1. Overview of Level 3. Information sharing in each Sector Group is among group members in that sector. Information sharing across sectors in the community is among Super Group representatives and Sector Group representatives from different sectors. A certain amount of information is shared with external entities (such as state and federal government) informally. Information shared in each Sector Group includes but is not limited to: threat indicators, warnings, alert or incident information, details about specific cyber incidents, and mitigation strategies. Physical evidences such as suspicious or unusual activity reports are also suggested to be shared. Aggregated alerts and threat indicators from different Sector Groups are shared with the Collaboration Group. Details and impacts of a specific incident, and mitigation plans are shared with the Incident Group related to this incident.

4.3.2. Maturity at Level 3. At this level the Super Group and the Collaboration Group are formally formed and a collaborative connection from all Sector Groups is established. A formal and secure information sharing mechanism is provided and formal information analysis is performed in the community. Incident Groups are dynamically created for managing specific incidents. The Super Group representatives start to share information with external entities (such as the state government and the federal government) informally.

- Technology Maturity: Basic group communication service is implemented in the Collaboration Group. (*e.g.* a mailing list with an additional repository for searching and query, Incident Groups can be presented as online sessions or discussion boards). Formal and standardized information formats are used in information exchanging (*e.g.* OpenIOC, IODEF, STIX, *etc.*). Professional information analysis is conducted by Super Group representatives on the collected information in the Collaboration Group with assisting tools and techniques. Metrics are defined for identifying an incident or potential threat to the whole community.
- Policy Maturity: Formal information sharing policies are defined, implemented and reviewed in each Sector Group and the Collaboration Group (including Incident Groups).
- Management Maturity: The Collaboration Group cyber threat analysts responsible for information analysis, incident coordination are appointed. An administration mechanism in the Collaboration

Group is developed. Administrators for the Collaboration Group are selected. In the Collaboration Group, the mechanism for admitting appropriate Sector Group and Super Group representatives into the Collaboration Group is established. The mechanism to manage Incident Groups and redirect an incident-related member to join an Incident Group is established.

An example of information sharing for a security-related event at Level 3 is given below:

Event 4.4: The utility sector representative reports 10 port scanning alerts from IP address 123.123.123.123 in his sector. This information is correlated with other information reported to the Collaboration Group. As more related information is gathered from across the community, a total of 100 port scanning alerts are received which reaches the predefined threshold to identify a threat to the community. The Super Group representatives perform information analysis and evaluation and provide mitigation guidance. This information is sent to other representatives in the Collaboration Group. The sector representatives disseminate this information to their sectors. An Incident Group is created for this event by a cyber threat analyst or an administrator of the Collaboration Group. Entities associated with this event will be redirected to this Incident Group for further sharing.

4.3.3. Effort to reach Level 4. The following effort should be done to reach the next level:

- Develop tools for group communication service satisfying real-time requirements and reliable message delivery. Develop tools for automated information gathering and information analysis.
- All group leaders should periodically review and update information sharing policies in that group, adding necessary additional policies for better security and privacy protection.
- The Super Group establishes information exchanging with the organization which provides local fusion (such as a local fusion center if it exists). If such an organization does not exist, the Super Group should develop techniques and tools to perform a certain level of local fusion, correlating and combining human intelligence and technical intelligence imported from internal and external sources.
- Super Group representatives periodically conduct surveys to evaluate he effectiveness of collaboration and security of information sharing.

4.4. Level 4 (Integrated)

4.4.1. Overview of Level 4. In addition to the previous level, information in the community is shared formally with the state and federal government according to state and national standards, it is also shared with other external entities such as neighboring communities. The shared information should include both evidence of cyber and physical incidents, both human intelligence and technical intelligence should be utilized. The fusion of cyber and physical intelligence is a major aspect of this level.

4.4.2. Maturity at Level 4. Formal information sharing and analysis is taking place internally and externally in the community. Formal local fusion occurs in the community. The effectiveness of collaboration and security of information sharing is reviewed and evaluated.

- Technology Maturity: A group communication service satisfying real-time requirements, providing reliable message delivery with automated information gathering is developed. Tools assisting automated generation and parsing of standardized information exchanging format is developed. Methodologies, tools and techniques are available to perform information analysis and local fusion, correlating human intelligence and technical intelligence related to the event.
- Policy Maturity: Information sharing policies are reviewed and updated with additional information disclosing and redistribution policies to external entities. More security and privacy protection is specified in the policies, *e.g.* update the security policy required for group communication to include a method to encrypt messages.
- Management Maturity: With the assistance of automation tools, the labor effort for management should be significantly reduced at this level.

An example of information sharing for a security-related event at Level 4 is given below:

Event 4.5: A policeman detects activities that could indicate a possible war driving event during a patrol. He may not realize this is related to a cyber event, so this information may not directly feed into the cyber security information sharing system. The location and time is reported to the police department, later this information is reported to the fusion center. An organization near where the police officer spotted the activities mentioned reports unusual network activity via the Collaboration Group. A Super Group representative reports this event to the fusion center. These two events are correlated and a threat is identified. Warning and

protection guidance is sent to other organizations that may be affected in the future.

One thing to be noted is that in earlier maturity levels, these two events may not be correlated since no local fusion service was provided. In such circumstances, the policeman's report may only be seen by the law enforcement agency. The two indicators are not able to be correlated if the policeman did not realize it might relate to a cyber event.

4.4.3. Effort to reach Level 5.

- If a fusion center already exists in the community, the Super Group representatives should establish information exchanging with the fusion center. Otherwise, the function and service comparable to a data fusion/analysis center should be provided by a specified organization and the Super Group representatives should collaborate with this organization.
- Develop techniques and tools to achieve a highly automated process of information exchanging and information analysis which correlates and combines cyber and non-cyber information from internal and external sources.
- All group leaders should periodically review and update information sharing policies in that group, adding necessary additional policies as needed.
- Enforce collaboration with more external information sharing entities across communities and develop formal communication methods and tools to communicate with external entities.

4.5. Level 5 (Vanguard)

This level, at the top of the CCSMM, involves considerable cyber capabilities and not all communities will need to reach this level. Whether a community needs to reach this level depends on the scale, the population, whether the community includes high value targets, and the cyber security capability of the major sectors in the community. Whether a fusion center needs to be established in this community also will need to be determined as it too requires a certain expenditure of city funds.

4.5.1. Overview of Level 5. In addition to the previous level, Super Group representatives exchange information with the fusion center and the EOC in the community. More external information sharing entities involved in collaboration across communities. The shared information should include all-source cyber and non-cyber information indicating a potential threat.

4.5.2. Maturity at Level 5. A fully integrated fusion/analysis center exists and is able to combine all-source physical and cyber information. A highly automated information sharing process is performed in the community. Effective collaboration with external entities is conducted.

- Technology Maturity: More advanced tools to achieve a highly automated process of information exchanging and information analysis is developed. A formal communication service with external entities is provided.
- Policy Maturity: Information sharing policies are periodically reviewed and updated with additional requirements as necessary.
- Management Maturity: Further reduce the manual effort in management and achieve high efficiency.

At this point Level 5 is only presented as a blueprint with a few visions of what it might entail and few details as much is not yet known about the level. As communities evolves towards this level much additional information will be needed to further define the level and what it entails.

5. Future work

The roadmap was presented to several security subject matter experts at the state and local level including individuals from the state of Texas's IT office as well as community IT and security experts. The overwhelming feedback was that this effort was valuable and needed and that in reality, a phased approach as shown in the previous section has the best chance of gaining support across the various sectors in the community.

As a mission to improve the Nation's cyber security posture by identifying standards and guidelines for effective cyber security information sharing and analysis, President Obama issued the 2015 Executive Order 13691 directing the DHS to encourage the development of Information Sharing and Analysis Organizations (ISAOs), including both industry and geographically-based ISAOs. This effort is led by the University of Texas at San Antonio with support from the Logistics Management Institute (LMI) and the retail Cyber Intelligence Sharing Center (R-CISC). This initiative validated the necessity of information sharing and collaboration from organizations and entities from private and public sectors. The form of such ISAOs is also group-based. The framework and evolution roadmap of this research could potentially serve as a blueprint on the creation of emerging organizations and management structures, for example, one can analogize the establishment of sector-ISAOs as Sector Groups, and a

geographical-based ISAO as a Super Group in communities. Currently, more than 100 experts from various industry sectors, government agencies, and academia have established standards working groups, which are now actively working on the standards and guidelines of the creation of ISAOs and information sharing. This effort, overlaps with much of the described effort in our evolution roadmap from Level 1 to Level 2. In the future, the ISAO initiative will potentially help facilitate much of the implementation of our blueprint in this paper and will collect and publish metrics reflecting the effectiveness of cyber security information sharing. Since the ISAO's standards and related documents are not yet published, whether they differ from our approach in certain details in terms of execution and implementation cannot be determined at this point. However, as the ISAO's future effort will be carried out in communities, our research will continue to refine our model and the information sharing maturity evolution process according to effectiveness of this process in communities. Our research also plan to explore or develop the technical mechanisms that will be needed to implement the automated information sharing when a community reaches higher maturity levels.

6. Conclusion

This paper presents the extended collaborative information sharing framework for community cyber security and discusses the most important aspects of information sharing. It also develops the Information Sharing Maturity Model for community cyber security as a roadmap with evolutionary procedures and incremental steps for community organizations to advance in their information sharing maturity. As an important part of the CCSMM model, this Information Sharing Maturity Model greatly enriches the CCSMM model. This framework and roadmap also potentially serve as a blueprint on the creation and development of emerging ISAOs. The evaluation of effectiveness of cyber security information sharing is included as ISAO's future effort, our research will continue to refine our model and the information sharing maturity evolution process according to such effectiveness in communities.

References

[1] "National cyber incident response plan." Homeland Security, sept 2010. [Online]. Available: http://www.federalnewsradio.com/pdfs/

[2] K. Gorzelak, T. Grudziecki, P. Jacewicz, P. Jaroszewski, L. Juszczyk, and P. Kijewski, "Proactive detection of network security incidents." European Union Agency for Network and Information Security (ENISA), 2011.

[3] P. Kijewski and P. Pawlinski, "Proactive detection and automated exchange of network security incidents," [Online]: http://www.cert.pl.

[4] J. H. M. W. Romain Bourgue, Joshua Budd and D. Kulawik, "Detect, share, protect - solutions for improving threat data exchange among CERTs." European Union Agency for Network and Information Security (ENISA), 2013.

[5] R. McRee, "Collective intelligence framework: A framework for warehousing intelligence bits," in *ISSA Journal*, 2012.

[6] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, and S. Adegbite, "Cybex: The cybersecurity information exchange framework (x.1500)," *SIGCOMM Comput. Commun. Rev.*, 2010.

[7] L. Dandurand and O. S. Serrano, "Towards improved cyber security information sharing," in *5th International Conference on Cyber Conflict*, 2013.

[8] G. White, "The community cyber security maturity model," in *IEEE Conference on Technologies for Homeland Security*, nov. 2011, pp. 173 –178.

[9] W. Zhao and G. White, "A collaborative information sharing framework for community cyber security," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, 2012, pp. 457–462.

[10] W. Zhao and G. White, "Designing a formal model facilitating collaborative information sharing for community cyber security," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, Jan 2014, pp. 1987–1996.

[11] N. Granado and G. White, "Cyber security and government fusion centers," in *Hawaii International Conference on System Sciences*, 2008.

[12] "Sophisticated indicators for the modern threat landscape: An introduction to OpenIOC," [Online]: http://www.openioc.org.

[13] J. M. R. Danyliw and Y. Demchenko. The incident object description exchange format. Network Working Group. [Online]. Available: http://tools.ietf.org/html/rfc5070

[14] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (STIX)." The MITRE Corporation, 2013.

[15] M. D. Julie Connolly and C. Schmidt, "The trusted automated exchange of indicator information (TAXII)." The MITRE Corporation, 2014.