WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING

DECEMBER 2016 Conduits for Information Sharing

Introduction:

CSRIC V Working Group 5 (WG5) is currently tasked with identifying and assessing existing conduits of information sharing in use across the industry. For this deliverable the Working Group was tasked with evaluating "available structures and platforms of Communications sector stakeholders to routinely share cybersecurity information (threat indicators and warnings, anomalous indicators, and post-incident information) within the constraints of existing law".

This document provides a summary of existing mechanisms by which information is exchanged both between private entities within the communications sector and with government building upon the previous reports on information sharing use cases, barriers and trust pools and will be included as the final chapter in the Working Group Final report to be released in March 2017.

For the purposes of this report the working group defined "conduits" as the following: a means by which something is transmitted[1]; a channel through which anything is conveyed[2]; an agency or means of access, communication, etc.[3] Based upon this definition there are many conduits for information sharing within the communications sector including ranging from informal items such as phone calls, emails, distribution lists to more sophisticated formal automated sharing such as that conducted by DHS. In its previous efforts to develop use cases, the working group found that information follows as a stream from informal to formal. Simple items such as phone calls or emails represent the most informal with automated machine to machine sharing representing the most formal arrangements.

Conduits for Information Sharing:

As noted above there are a variety of mechanisms for sharing information ranging from informal items such as a phone call, email, distribution list, teleconference, meeting, briefing, professional membership, working group, professional conference, webinar, technical liaisons, technical seminars or conferences, tabletop exercises to more formal items such as automated information sharing. Table 1 below lists the various forms of information sharing ranging from informal to formal:

Table 1: Mechanisms for information sharing from informal to formal

Informal

Phone Call
E-mail
Teleconference
Professional Membership
Working Group
Professional Conference
Webinar
Technical Liaison
Technical Seminar or Conference
Tabletop Exercise
Full Scale Exercise
Automated Sharing

Formal

[1] American Heritage Dictionary of the English Language, Fifth Edition. Copyright © 2011 by Houghton Mifflin Harcourt Publishing Company. Published by Houghton Mifflin Harcourt Publishing Company. All rights reserved.
[2] Random House Kemerman Webster's College Dictionary, © 2010 K Dictionaries Ltd. Copyright 2005,1997, 1991 by Random House, Inc. All rights reserved.
[3] Collins English Dictionary—Complete and Unabridged, 12th Edition 2014 © HarperCollins Publishers 1991, 1994, 1998, 2000, 2003, 2006, 2007, 2009, 2011, 2014

A **telephone call** between two people who may be business acquaintances is the most informal way of sharing information. A phone call would be used in a situation where basic information should be shared, i.e., whether either party is aware of open source reporting (i.e., on the radio or television) about a cyber-attack and whether the attack affects them.

Using **electronic mail** between the two parties is the next most informal avenue. An email could be used when the two parties wish to share slightly more detailed basic information, i.e., one organization wishes to share information to remedy a type of cyber-attack with another related to a specific cyber-attack which affected one organization and may have affected the other organization. Of course information sharing through email can be transmitted from one to several parties or more formally through a distribution list of participants. When more than one organization is involved in the specific cyber event, information regarding the event and precautions or practices to alleviate the issues resulting from the event can be shared among trusted partners. This occurs when members of a trust pool contact each other and a government entity.

These participants can take the information sharing to a concerted organizational level through a designated bridge for a **teleconference**. A teleconference may be convened when a cyber or physical event requires discussion and coordination among the affected parties, whether industry or government entities. The next step would be a face to face meeting among participants. At a briefing, a subject matter expert could share information with several participants with a need to know and a shared understanding. A meeting or briefing may occur to provide information to participants because of an event or in anticipation of an event to coordinate organizational activities which may affect a large population.

Professional membership in an organization, i.e., one of the recognized trust pools, provides a more concentrated focus. Information sharing through professional membership occurs when some, most or all members of the profession may be affected by an event. A **working group** -- an ad hoc group of subject matter experts in the same industry working together to achieve specified goals -- may come together regarding a domain and focus on discussion or activity around a subject area.

At a **professional conference**, subject matter experts may share information pertaining to their profession as well as a cyber or physical event. Because all the professionals may not be available to attend a conference, a webinar-- a seminar or other presentation that takes place on the Internet allowing participants in different locations to see and hear the presenter, ask questions, and sometimes answer polls -- also provides a means for the information sharing process. A **webinar** may be initiated to provide professionals with best practices or lessons learned as the result of a cyber-attack.

In a **technical liaison relationship**, a subject matter expert from an organization provides technical expertise to communicate and coordinate activities, i.e., share cybersecurity information, with another organization with the goal of resolving an issue or event. Technical liaisons generally occur in conjunction with a cyber event or may be initiated because of a cyber event. The organization's liaison officer may be collocated at a security operations center as part of a memorandum of agreement between the organization and the center.

A **technical seminar or conference** may be convened to discuss an event or issue among liaison officers. Such a seminar or conference may occur because of one or more cybersecurity events affecting several critical infrastructure organizations and government entities. Because this type of information sharing

opportunity may require extensive collaboration and coordination, lead time for this activity may be several months after the occurrence of the event or issue.

Thus, or because of the likelihood of a cybersecurity event, a **tabletop exercise** involving executives of various organizations and government entities may provide strategic information sharing. A **full scale exercise** involving likely affected organization liaison officers and government entities provides the best opportunity for practicing the information sharing process. As with the technical seminar or conference, a tabletop or full scale exercise may require several months to a year to organize and execute.

The ultimate means of sharing cybersecurity information and the most formal would be an organization's application for membership in and use of an **automated information system** such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). STIX and TAXII are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time notification and response. Information shared through an automated system is validated before distribution.

Information Sharing Examples:

The following are a few real world examples of information sharing using industry and government entity. In the first example, an industry engineer discovered the Heartbleed vulnerability and after, committing and applying a patch, shared the information with an international organization via email. The international organization used a distribution list to send out an advisory sharing the information. A government entity used the advisory to post a technical alert to its portal, to which trusted partners had access. Information regarding this vulnerability led to convening a trust pool members' meeting and associated teleconference. To further share information about the vulnerability, a government entity used a distribution list to request information on confirmed exploits from trust pool members. Once the vulnerability was patched by more affected government and industry partners, another government entity conducted webinars on the vulnerability, sharing analysis and mitigation actions.

In another example of the information sharing process, a foreign government's commercial banks and government agencies experienced heavy distributed denial of service attacks from over 150 countries and contacted its government computer emergency response team. The foreign government computer emergency response team (CERT) contacted by email through an international cyber organization distribution list the US Computer Emergency Readiness Team for mitigation assistance, providing the pertinent attacking information for cross data analysis. US-CERT notified via email another US government entity, the Communications ISAC, which in turn contacted the potentially associated sector members via email. Sector members researched and identified the problems and implemented mitigation strategies to alleviate the attacks. Once mitigation was completed, the US-CERT emailed and telephoned the foreign government CERT to ensure the activity had ended.

Information Sharing Challenges:

There are some challenges related to sharing information most of which result from scalability concerns. These issues appear to shape the cybersecurity information sharing processes for the Communications sector. Table 2 Challenges and Scalability, provides lists of proactive and conflicting issues which the working group recognizes.

Table 2: Challenges and Scalability

PROs	CONs
Established trust pools support through personal relationships	Small to medium sized businesses may have neither cyber personnel nor capital to expend
Use cases provide evidence of previous info sharing activity and substance for increasing and improving incident response	Desired degree of information sharing attention may not be realized until cost benefit can be justified for SMBs
Use cases include annual cybersecurity incident study, incident responses and various exercises involving private sector and/or government entities at state, regional, national, and international levels	Need for additional cybersecurity personnel will strain availability as more private sector/government entities participate, especially personnel with security clearances
For networks with less (relative) traffic, anomalies/incursions may be easier to detect, thereby shrinking operator and industry response time	

The list of issues above is not intended to be all inclusive but highlight some of the main challenges identified by the Working Group.

Future Activities:

With all private sector partners, and especially in the case of small to medium sized businesses (SMBs), capabilities or resources to fully engage in a two-way information sharing process is dependent on cost effectiveness and workforce availability for each business. Most SMBs may only participate as consumers of information through informal means (personal/professional relationships) instead of formal means (organized trust pools which cater to larger private sector partners). Some SMBs might not participate at all and, therefore, may be blind to any external cybersecurity information.

The creation and increased use of Information Sharing and Analysis Organizations (ISAOs) and the establishment of the ISAO Standards Organization in October 2015, should improve the nation's cybersecurity posture within SMBs. ISAOs may provide an information sharing outlet between the government and SMBs which might not participate in formal, more organized information sharing trust pools. The ISAO Standards Organization may help with this effort by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.[4]

For their part, government entities and larger private sector partners may continue to use the identified trust pools and the array of cybersecurity legislation and guidelines to further enhance and refine information sharing processes. As necessary, additional trust pools, cybersecurity legislation[5], [6] and

[4] ISAO Standards Organization, https://www.isao.org/ viewed 19 August 2016.
[5] U.S. law enforcement and intelligence officials said on 15 September 2016, they are building legal cases to respond to growing Russian attempts to disrupt and discredit the November elections without sparking an open confrontation with the Russian President. See http://www.reuters.com/article/us-usa-cyber-russia-idUSKCN11M00H, viewed 19 September 2016.
[6] The National Bank of Belgium, the New York Fed, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) this summer set up a task force with representatives from some 25 central banks to set cybersecurity standards around inter-bank transfers that may be adopted globally. The new principles or guidance could cover responsibilities of banks that send and receive money transfers and networks like SWIFT that transmit payment instructions in correspondent banking. This is in response to the 81 million dollar Bangladesh bank heist. See http://www.reuters.com/article/us-cyber-heist-basel-taskforce-idUSKCN11L269, viewed 19 September 2016.

other guidance may evolve to further define and refine the cyber environment and, in succession, information and the sharing processes. Human to human information flow processes may continue to be supplemented with machine to human information flow processes. Machine to machine information flow processes also may be added as the cost or benefits are discovered and the value of and need for additional information flows are realized and incorporated as part of the business model for all entities.

Technology

Finally, the working group discussed the various technologies available to facilitate information sharing. For information flow processes involving machines, available structures and platforms include automated information systems (AIS), such as Structured Threat Information eXpression (STIX), and Trusted Automated eXchange of Indicator Information (TAXII). STIX, a collaborative effort to develop a standardized, structured language to represent cyber threat information, conveys the full range of potential cyber threat elements and strives to be expressive, flexible, extensible, automated and human-readable. TAXII, a set of services and message exchanges, empowers organizations to share the information they choose with partners they choose.[7] These technological means have the potential to be instrumental in sharing information among private sector and government entities. However, the working group finds, while the technology is beneficial, it is still developing and it appears only larger businesses and government entities have begun to take advantage of the benefits and allocated the workforce.[8] SMBs remain inhibited by cost/benefit and resource constraints.

[7] Information Sharing Specifications for Cybersecurity, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity, viewed 30 Aug 2016.

[8] As of 27 Sep 2016, about 50 agencies, private companies and organizations have joined the DHS automatic information sharing network, STIX/TAXII. http://federalnewsradio.com/cybersecurity/2016/09/dhs-50-agencies-private-companies-cyber-information-sharing-network/, viewed 28 Sep 2016.