Regional Cybersecurity Situational Awareness Project Workshop

Summary Report

June 18, 2018 | 8:30 - 11:00AM
Seattle Police Department Headquarters

Executive Summary
The Cybersecurity Situational Awareness Project workshop was held on June 18, 2018, in Seattle, Washington, at Seattle Police Department Headquarters. This was the second workshop held for this project, and focused on further developing and refining a Concept of Operations (CONOPS) for cyber incident reporting for the Puget Sound area. At the workshop, participants were invited to provide input on the latest draft CONOPS. The first workshop focused on input from stakeholders for the development of an initial draft CONOPS.

Background
The purpose of the Cybersecurity Situational Awareness Project is to create a clear process and method for reporting cybersecurity incidents, enhance situational awareness, and foster a regional information and resource sharing community across jurisdictions and sectors. The overarching goal of the project is to develop a Concept of Operations (CONOPS) for a standardized regional reporting method for significant cyber incidents and to define the who,what, when, and where of that process.

Since the last project workshop in March, the scope of the project was expanded to include all critical infrastructure sectors within the region. The project initially focused specifically on the maritime industry, but the project scope now includes all regional partners involved in critical infrastructure sectors.

Workshop participants took part in the following:

- Discussed and provided input on the latest draft version of the Puget Sound Region Cyber Resilience CONOPS
- Helped in crafting the process for the reporting of significant cyber incidents in the region

- Discussed definition of the thresholds for what constitutes a significant cyber incident
- Discussed with other regional stakeholders on expectations and best methods for sending, receiving, and sharing information during and after the reporting of cyber incidents

Purpose of CONOPS

The purpose of the Cyber Resilience CONOPS is to enable the sharing of information and analysis that can assist state, local and tribal agencies, and public and private sector critical infrastructure providers and key resource stakeholder organizations in the performance of their public safety, security, continuity, and disaster resilience responsibilities. This CONOPS focuses on Cyber Security Incident reporting and response in Washington State. It suggests processes, protocols, and policies that any stakeholder organization can put into practice to increase their resilience and response capabilities before, during and after a serious cyber security incident. It includes suggestions for tools and specific guidelines by which an organization will be able to better detect, triage, and respond effectively to a cybersecurity intrusion or compromise. It specifically includes guidance for engaging with the local cyber community, including public and private sector partners, law enforcement, and State and Federal resources.

Summary of Workshop and Stakeholder Input

Andrew Whitaker, Chief Information Officer for City of Seattle, opened the workshop by welcoming participants and explaining the importance of developing a standard protocol for reporting cyber incidents within the region. Whitaker presented stakeholders a current assessment of the cyber threat landscape. Whitaker emphasized that information sharing is a key to increasing resiliency within the regional cyber realm. New technologies have opened up new opportunities for bad actors and new vulnerabilities for cyber infrastructure. Technologies such as wearable tech, the Internet of Things, and integration of smart tech assistants like Cortana and Alexa into businesses are all examples of these new vulnerabilities. Cyber attacks are becoming increasingly common among smaller organizations and municipalities that do not have the ability to combat them. Historically, cybersecurity was about protection against attacks. However, the mindset for cybersecurity needs to shift towards detection of and response to threats.

Following the discussion of the current cyber threat landscape, David Matthews, project consultant, led participants through a review of the CONOPS. Participants provided verbal feedback and were invited to provide additional written input. The stakeholder input will inform the next steps of the process.

It was noted that circumstances might change and there may be a need to amend the CONOPS based on events that may influence new policies and requirements at the Federal, State, and Local levels. The CONOPS will be voluntary for all participants. The development of the CONOPS is being undertaken in an effort to produce a general, but detailed document that can be applied across a broad range of industries, organizations, and situations. While it was acknowledged that some industries have specific regulatory reporting requirements, there is still a need to produce a one-size-fits-all document providing a general standardized reporting methodology for cyber incidents. Currently not statewide guidance exists and there is no clear path for reporting. It was noted in the survey that groups identified half a dozen agencies they report to and most were at the federal level leaving out the local and state government and law enforcement.

The Washington State Fusion Center has agreed to be the central entity to report to for cyber incidents. Sergeant Deb Windsor of the Fusion Center gave an overview on the Fusion Center's current role within the State, their role within the project, and the importance of having a systemized and clearly defined reporting process. A standardized process is important for the purpose of collecting and disseminating information. The Fusion Center will serve in this capacity. Participants discussed the best methods for reporting information, and expectations for receiving reports and information back. It was noted that the Fusion Center is not a 24/7 operation and is grant funded. The Fusion Center noted that they would like to made aware of all incidents, regardless of severity level, to gain better situational awareness of the current threat landscape.

Participants discussed several ways of reporting to the fusion center including online forms, phone messages, email and a possible app. Participants had no clear one size fits all method for reporting and each had reasoning for their preferred method. It was noted that participants could pre-populate the forms in the appendix to make reporting quicker and more streamlined. Some did not want to email a report because it becomes public record and would rather report through a website or app or call. As we continue to develop the CONOPS we will explore how to incorporate multiple reporting methods and later test these to determine the best path forward.

It was noted during the discussion that reference to NIMS/ICS should be removed since the current nation cyber guidance does not follow NIMS/ICS. This model does not mesh well with emergency management and law enforcement response planning. It was noted that most often the private sector does not follow NIMS/ICS as well and that the conops should not try to force participants into a particular model during an incident.

Several discussions revolved around privacy and classified information. The Fusion Center is not an original classifier of information. They do anonymize information as it is shared. Concerns were raised that sending information to a government agency make it subject to public disclosure laws. There is an exemption on public access for any information that reveals a vulnerability. It was suggested that the CONOPS include the citation of the Revised Code of Washington (RCW) about protecting vulnerabilities.

Stakeholders suggested that a list of all currently now available resources and authorities be added to the CONOPS. It was recommended that the document clarify that reporting entities understand that they are only submitting a report and that responsibilities and authority remains with the reporting organization.

Participants asked how we might explore incorporating machine to machine collection and reporting in real time as a future add-on to the CONOPS. Most agreed that the first step is to create the basic path to report and then move toward a more sophisticated method of reporting and response coordination and assistance. Several participants noted the importance of relationships and trust and the need to find opportunities to meet and understand the needs of stakeholders. The best path toward increasing resilience is by improving information sharing across all sectors and jurisdictions. The best way to do this is to encourage stakeholders to report and ensure useful information is returned by the fusion center.

Several stakeholder asked about what level of reporting is really needed. Several thought routine incidents should not be reported. The fusion center however stated they would like all levels, including phishing attempts. It was noted that the analyst at the fusion center spends the majority of his time focused on detecting phishing trends and trying to shut down similar attempts across the region. It was noted that the fusion center may not act or provide responses on every phishing reporting but they do log and analyze specific trends. This helps provide better intelligence and warnings to other similar sectors and infrastructures. Bottom line, they would like everything. It was noted that an ideal situation would be to have a server available to upload files and allow analysts to access and look for trends related to the data. Currently there is no repository for uploading logs and other data. A regional database that could be shared across states would be a useful asset in the future. This would also allow states with less of a cyber presence in their fusion center to take advantage of the ability of a neighboring jurisdiction’s analytical capability.

The co-chair of CIRCAS (Cyber Incident Response Coalition & Analysis Sharing) noted that references to CIRCAS as an organization should be removed because it is not an official response asset. While it is referenced as a state-wide asset in the WA Cyber

Response Framework, it isn't an on call assisting body. It was noted that CIRCAS plays a key role in providing advice to the state and beyond, but it has a ways to go before it can be considered a voluntary reserve corps standing ready to assist. More work should be done to explore how we can officially recognize CIRCAS in this capacity.

Following the final draft of the document, a tabletop will be held later in the fall to test the final CONOPS. The date for this exercise is set for September 12. More information will be distributed to stakeholders as the date approaches.

Next Steps and Timeline:
1) Revise CONOPS per the verbal and written stakeholder input received
2) Send out updated CONOPS to stakeholders group for continued comments
3) Host exercise testing and develop final CONOPS

Appendix:
Agenda

Workshop Agenda
Regional Cybersecurity Situational Awareness Project Workshop

June 18, 2018 | 8:30am – 11:00am
Seattle Police Department Headquarters | Training Room

The purpose of the Cybersecurity Situational Awareness Project is to create a clear process and method for reporting cybersecurity incidents, enhance situational awareness, and foster a regional information and resource sharing community across jurisdictions and sectors. The overarching goal of the project is to develop a Concept of Operations (CONOPS) for a standardized regional reporting method for significant cyber incidents and to define the who, what, when, and where of that process. For more information on this project, visit www.regionalresilience.org/cybersecurity-situational-awareness-project.

Welcome, Introductions, and Overview

- Brandon Hardenbrook, PNWER

Briefing on Current Cyber Threat Landscape

- Andrew Whitaker, Chief Information Security Officer, City of Seattle

Overview, Input, and Discussion on Draft CONOPS

- David Matthews, Project Lead Consultant

Discussion on Upcoming Exercise to Test CONOPS – September 12

- Eric Holdeman, Director, Center for Regional Disaster Resilience

Wrap-up and Next Steps