Cybersecurity Incident Reporting Exercise

Summary Report

September 12, 2018 | 8:00AM - 1:00PM
DoubleTree Suites Airport - Southcenter | Seattle, WA

Executive Summary
The Cybersecurity Incident Reporting Exercise was the final of three events held as part of the Cybersecurity Situational Awareness Project and was designed to gather final feedback for and exercise the draft cyber incident reporting Concept of Operations (CONOPS) created to develop a standardized process for cyber incident reporting within the region. The project is funded by the US Department of Homeland Security as part of the National Infrastructure Protection Plan Challenge Grant Program.

The Cybersecurity Incident Reporting Exercise convened a broad cross-section of public and private stakeholders to address this issue. During the exercise stakeholders participated in several scenarios on cybersecurity incidents, ranging in severity from minimal to significant incidents, in order to exercise the draft CONOPS. Attendees were asked to provide feedback on the CONOPS and the process of reporting cyber incidents. Following the incorporation of exercise feedback and stakeholder input, the finalized CONOPS will be released.

Rep. Zack Hudgins speaks to exercise participants about the importance of working together to protect against cyber threats

In addition, attendees heard remarks from Rep. Zack Hudgins, Washington State House of Representatives, and a panel discussion on election infrastructure security with Patrick Massey, Region X Director, Department of Homeland Security, and Julie Wise, Director of Elections, King County.

Background

Over the past several years stakeholders have consistently identified a major gap in cybersecurity preparedness in several exercises and workshops. The lack of a cohesive, standardized process for reporting cybersecurity incidents as the state and local levels was consistently one of the top issues identified. Numerous resources and outlets are available at the federal level, however, there is a no clearly identified process for organizations that have been targeted on who, what, where, and when to report at the local and state level. In addition to a lack of clarity around the specifics of reporting, expectations on how, where, and when the reported information is disseminated remains unclear. The CONOPS seeks to address questions such as these and serve as a starting document in the process to further clarify the reporting process and create a more resilient cyberinfrastructure in Washington.

A major product of the project was the development of a stakeholder self-assessment tool and survey, which was designed in order to help develop a baseline of current best practices and investments in cybersecurity in the region. This serves as an excellent self-assessment tool that allows organizations the ability to measure the maturity of their current cybersecurity resilience and response capabilities.

https://www.regionalresilience.org/cybersecurity-situational-awareness-project.html

The Cybersecurity Situational Awareness Project is funded by a grant through the Department of Homeland Security (DHS) and implemented by the Pacific NorthWest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR).

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 cybersecurity 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.

Opening Remarks from Rep. Zack Hudgins

Representative Zack Hudgins, Chair of the State Government, Elections and Information Technology Committee, Washington State House of Representatives, provided opening remarks. As chair of the Committee, which, among other issues, focuses on information technology systems and security, Rep. Hudgins also sits on the House Committee on Technology and Economic Development and is keenly aware of the importance of developing a strong cyberinfrastructure in the state of Washington. Rep. Hudgins noted that cybersecurity is an ongoing and ever-evolving field, and in today's interconnected world, cybersecurity and protecting infrastructure is more important than ever. Smart policy has much to do with protecting our cyber infrastructure. Engaging with legislators and ensuring that they remain informed of the issues is important to developing policy that is conducive and provides all with the tools and capabilities to combat cyber threats.

Rep. Hudgins acknowledged that work that PNWER and the CRDR have done on the topic of cybersecurity, including the Emerald Down cyber exercise series looking at emerging issues and relationship building in the regional cyber realm. Rep. Hudgins thanked the efforts of those in the room for seeking to find solutions and protect against cyber threats.

Patrick Massey, DHS Region X Director, and Julie Wise, King County Director of Elections, speak on election infrastructure security

Overview of CONOPS - David Matthews

David Matthews provided an overview of the process over the past year to develop the CONOPS. We initially formed an advisory group to assist in steering the project and to provide input on the development of a survey and self-assessment tool. The Coast Guard played a significant role in getting this project off the ground. The last district commander stated that this issue was his number one priority and wanted to get stakeholders to work together to define what a cyber incident is and who to report it to. The USCG has made significant progress on this issue over the past year. As we progressed on the progress we quickly realized that this is beyond the maritime sector and many stakeholders asked us to expand the scope to include all sectors. DHS agreed with this and allowed us to open this up to all sectors. Many groups have played a leading role in this effort, especially the Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) group. This group also has helped spur on the need for more information sharing across sectors and is

working to build a network of trusted professionals who can assist each other. This message is an important theme throughout the CONOPS.

The Fusion Center and WA Military Department both provided comments on the importance of ensuring local and state agencies are aware of cyber incidents. This will increase the overall readiness and resilience of the region. The Fusion Center is working to share information about potential threats and the state is ready to provide incident response assistance in the event of a significant cyber incident. The state has already developed NIMS typing for cyber resources and is ready to provide assistance when called upon.

It was recommended that when laying out reporting to Fusion Center, entities should be proactive to define individuals responsible for taking care of sending a report and pre-staging what to do. It is recommended to pre-define who is in charge, and who will make the report and follow up on the report. This will help the fusion center recognize the lead. Once the report is submitted through various methods, the conops lays out the process of analyzing and sharing the information. It also lays out how do we archive this information for the future, and how do we disseminate the information.

There is a severity rating matrix that you can use for your own organization to help determine when to report. There is also a template you can use to pre-populate with your critical information to help speed up the process.

Remarks from the Washington State Fusion Center
Erik Allen, Deputy Director, Washington State Fusion Center, spoke on the role of the Washington State Fusion Center within the State, and, more specifically, within the Cybersecurity Situational Awareness Project. The Washington State Fusion Center serves as a key partner in the Project and PNWER, agreeing to be the single point of contact, as identified in the CONOPS, to whom cyber incidents would be reported to and information would be disseminated from. Allen reinforced the importance of standardizing the method for cyber incident reporting and exercising the methodology.

Allen provided an overview of the Fusion Center and its mission to support public safety and security of state, local, tribal, and private sector entities, by providing information and intelligence. The Fusion Center works to overcome problems of information sharing. The Fusion Center has been looking at the issue of cyber for several years. One of the Fusion Center's listed objectives is to "Provide Cybersecurity Awareness". The Washington State Fusion Center is operated out of the FBI Building in Seattle, and pulls together individuals from a number of organizations at various levels of government, including DHS, FBI, and city and state law enforcement.

Allen noted the limited capacity and small size of the Fusion Center but emphasized that if they serve as a place to ask questions of and seek answers. If they do not have the answer, they have the resources and relationships to know where to go to seek the answer.

Tabletop Incident Scenarios and Report-out

The CONOPS was exercised through several incident scenarios ranging in severity from minimal to significant. Stakeholders were seated in mixed tables of sectors and jurisdictions for the discussion. Each table had a facilitator and note taker to capture key points.

Scenario #1

In a large organization, your network administrator notices a large increase in outbound traffic from your personnel database during routine monitoring of network traffic.

Scenario 1 Takeaways

- In order to maximize efficiency and minimize response time, contracts should be in place between State and public organizations. Contingency discussions and pre-established agreements should be established so that time would not have to be spent negotiating a contract if something were to happen. It was suggested that interested parties reach out to the Washington Office of Cybersecurity for more information. The City of Tacoma has several contracts and resources in place that are leveraged on a regular basis.
- Establish a clear phone tree for emergencies and up-to-date organizational structure prior to incidents occurring.
- Make employees aware of important entities to call during emergencies, such as the Fusion Center, MS-ISAC, etc.
- There should be a clear list of available resources listed in the CONOPS.
- Organizations should make introductions with fusion center staff to begin to build relationships and trust.
- Organizations should ask to receive the fusion center's weekly cyber update email regarding cyber threats and other news.

Scenario #2

Friday, mid-morning an employee in the finance department of your organization turns on their computer and finds a ransomware demand. Their computer and all connected resources have been encrypted and the demand is for bitcoins to pay for decryption codes.

Scenario 2 Takeaways

- Establishing relationships, building trust, and providing incentives for information sharing are key. When sharing information, will organizations receive information back? Will the information sharing be reciprocated?
- The Fusion Center wants to be made aware of every all phishing email, ransomware, etc. Do not assume it is too routine to report.
- Information such as bitcoin addresses greatly helps track these types of attacks

- Know your organization's incident response plan. Share with your employees Maintain a hard copy, because if networks are down, these files are not accessible.
- Maintain good backups and regularly backup systems.
- Know how to communicate with employees during incidents. If systems go down and access to email is not possible, then there needs to be a clear communication method among leadership and employees. Know what to tell employees and be able to clearly communicate to them what to do in the situation.
- C-Suite executives should be kept up-to-date regarding incidents. However, be able to prioritize information, and be aware of their decision making process and rationale.
- Be honest regarding incidents. Full disclosure, when appropriate, is best.

Panel Discussion

Scenario #3

You are working with a water utility organization – Over the weekend, your systems management receive alerts that one of your control systems has alerted. Preliminary investigations indicate it was caused by a malware infection.

Scenario 3 Takeaways

- Be aware of health regulatory requirements when delving into incidents that involve public health, i.e. public utilities.
- Building relationships with organizations/utilities is key. In doing so, you are creating a trust that makes organizations/utilities more willing to share information during incidents and keep you in the loop.
- Isolate issue, verify what is happening, and understand the significance of the incident.
- Incidents with possible impacts to public health need to have a minimum and low threshold for reporting because of the serious implications to the public.
- Start thinking about crisis communications. During major incidents, what is the messaging that will be shared with news organizations and publicly? To whom should this messaging go to? Thinking ahead of time about messaging is beneficial.

Scenario #4

As you are investigating the former scenario, many systems suddenly fail creating a catastrophic failure of your ability to perform critical infrastructure requirements.

Scenario 4 Takeaways

- Be aware of interdependencies and cascading effects of significant incidents.
- A risk assessment of the water sector that includes an analysis of interdependencies should be conducted on a regional level. This should include cyber risk and a regional

impact analysis. Water touches many different sectors and many parts are unregulated and many small water resources do not have IT staff.
- Are there mutual aid agreements that can be pre-established in order to expedite response time and clarify roles and resources during incidents? Do public organizations have cyber mutual aid agreements or can current emergency management mutual aid be used in a cyber attack?
- Understand when an incident extends beyond cyber and needs to be treated as disaster response, as in the case of critical infrastructure breaches.
- Exercise, exercise, exercise
- Events like this help develop relationships and uncover interdependencies, we need to encourage more investment in activities to build trust across the region.

Election Security Panel

Patrick Massey, Region X Director, Department of Homeland Security, and Julie Wise, Director of Elections, King County, participated in a panel on the security of Election Infrastructure. In light of recent events and increased scrutiny on protecting US elections against outside interference, election infrastructure security has emerged as an extremely relevant topic. In January 2017, election infrastructure was designated to be a national critical infrastructure as a subsector of Government Facilities. Panelists informed attendees and answered questions on the efforts being made to protect elections at both the national and local level. The panel was moderated by CRDR Director Eric Holdeman.

As defined by DHS, election infrastructure refers to assets, systems, and networks most critical to the security and resilience of the election process, such as storage facilities; polling places; voter registration databases and supporting systems; and infrastructure and systems used to count, audit, and display election results. DHS focuses on cyber and physical threats to these infrastructures and systems. DHS currently works with a variety of state and local partners in this capacity of providing support and services to the election infrastructure community. The value of protecting election infrastructure is emphasized by understanding that typical county elections officials could be managing more technology than the county IT department.

On a more local level, King County Elections Director Julie Wise provided an overview of King County's election process, infrastructure, and security measures. King County has been recognized as one of the best counties in the country for protecting election infrastructure. King County stands as the 13th largest county in the nation, encompasses 1.3 million votes and 191 jurisdictions, and is the largest county to vote exclusively by mail-in ballots. Mail-in ballots provide a paper trail for elections.

Wise mentioned that protecting election infrastructure includes both physical security and system security. Regarding physical security, King County undertakes numerous measures to protect the elections facility and ballots. These measures include 22 security cameras monitored 24/7, live-streaming via 6 webcams during ballot processing, restricted badged access to ballot processing areas, and additional biometric and badge required access. Systems, or cyber,

security measures include isolating systems so that databases are separated from tabulation systems, making the tabulation system closed-network, requiring physical access in order to be able to tamper with systems, and implementing the aforementioned physical measures in order to prevent physical access to systems.

In addition to these physical and systems measures, King County Elections and Wise look to continually increase security and reduce vulnerabilities. Wise asked DHS to conduct an assessment of King County Elections' physical security, which was completed in November 2017. A security analysis was also conducted by DHS and completed in June 2018. An outside audit was also conducted in late 2017 to examine the cybersecurity of the infrastructure. King County Elections regularly works with other state and federal agencies to ensure security threats are proactively addressed. Wise noted that it is not possible to do everything alone, and it is, therefore, critical to build partnerships.

Questions arose regarding efforts to combat disinformation and social media influence by nation-states. Massey responded that there is a federal task force that was created to look at that issue. Wise stated that we need to make sure that we have secure elections at the federal level and that there is support by legislators to do everything possible to protect election infrastructure.

Appendix A: Agenda

Cybersecurity Incident Reporting Exercise Agenda

September 12, 2018 | 8:00am – 1:00pm
DoubleTree Suites Seattle Airport – Southcenter | Seattle, WA

8:00AM **Registration**

8:30 **Welcome and Introductions**

- Eric Holdeman, Director of Center for Regional Disaster Resilience, PNWER

8:40 **Welcome from Rep. Zack Hudgins, 11th District**

8:55 **Overview of CONOPS**

- David Matthews, Project Consultant, PNWER

9:20 **Opening Remarks from Washington State Fusion Center**

- Erik Allen, Deputy Director, Washington State Fusion Center

9:30 **Tabletop Scenario #1 and #2**

10:10 **Break**

10:25 **Panel Discussion #1: Perspectives on Reporting and Response**

- A. Barrett Adams-Simmons, Regional Sector Outreach Coordinator, Department of Homeland Security
- Lance Fuhrman, Cyber Intelligence Analyst, Washington State Fusion Center
- Robert Lang, Cyber Security Manager, Washington Military Dept.

10:45 **Tabletop Scenario #3 and #4**

Panel Discussion #2

12:00 **Break for Lunch**

12:15 **Election Security: The Cybersecurity of Our National and Local Election Infrastructure**

- Patrick Massey, Region 10 Director, Department of Homeland Security
- Julie Wise, Director of Elections, King County

1:00 **Adjourn**

Appendix B: Exercise Scenarios and Questions

Scenario #1

In a large organization, your network administrator notices a large increase in outbound traffic from your personnel database during routine monitoring of network traffic.

1. To whom would they report this event? Would they know?
2. Who would triage and resolve the event?
3. Who would be notified inside your organization and with what priority and frequency?
4. What would be the threshold where you would feel it important to report outside your organization?
5. Are there regulatory requirements to report?
6. Who would be notified outside your organization – how and what information would be shared?
7. Would you have access to outside assistance? How and from whom?

Scenario #2

Friday, mid-morning an employee in the finance department of your organization turns on their computer and finds a ransomware demand. Their computer and all connected resources have been encrypted and the demand is for bitcoins to pay for decryption codes.

1. To whom would they report this event? Would they know?
2. Who would triage and resolve the event?
3. Who would be notified inside your organization and with what priority and frequency?
4. What would be the threshold where you would feel it important to report outside your organization?
5. Are there regulatory requirements to report?
6. Who would be notified outside your organization – how and what information would be shared?
7. Would you have access to outside assistance? How and from whom?

Scenario #3

You are working with a water utility organization – Over the weekend, your systems management receive alerts that one of your control systems has alerted. Preliminary investigations indicate it was caused by a malware infection.

1. To whom would they report this event? Would they know?
2. Who would triage and resolve the event?
3. Who would be notified inside your organization and with what priority and frequency?
4. What would be the threshold where you would feel it important to report outside your organization?
5. Are there regulatory requirements to report?
6. Who would be notified outside your organization – how and what information would be shared?
7. Would you have access to outside assistance? How and from whom?

Scenario #4

As you are investigating the former scenario, many systems suddenly fail creating a catastrophic failure of your ability to perform critical infrastructure requirements

1. To whom would they report this event? Would they know?
2. Who would triage and resolve the event?
3. Who would be notified inside your organization and with what priority and frequency?
4. What would be the threshold where you would feel it important to report outside your organization?
5. Are there regulatory requirements to report?
6. Who would be notified outside your organization – how and what information would be shared?
7. Would you have access to outside assistance? How and from whom?
8. What are your organization's interdependencies in this scenario?
9. Will you relocate? At what point will you relocate?"
10. At what point do you make public the cause of impact?

Appendix D: Feedback Form

Overall impression and general comments on the exercise- Please rate each component on a scale of 1-5 (5 being excellent /valuable; 1 being not valuable)

Workshop	Excellent	Very Good	Satisfactory	Fair	Poor	N/A
Overall Impression of Workshop	5	4	3	2	1	N/A
Quality of Workshop Speakers	5	4	3	2	1	N/A
Workshop Format	5	4	3	2	1	N/A
Quality of Discussion	5	4	3	2	1	N/A

1. What industry or type of organization do you represent? (e.g., Emergency Services; Law Enforcement; Energy; Local, County, State, Federal Government, Utility, Private Sector and type of business, etc)

2. What was the most useful aspect of the exercise? Presentations; Table Discussions

3. What was the most valuable 'take away' or insight you gained from today's activities?

4. Based on the presentations and discussion today, list any areas that were identified that you think could be improved at your organization, the state, or the region:

_____
_____
_____

5. What organizations and sectors, not here today, should be part of future meetings and workshops? (Please include contact names and information if available.)

6. What revisions or additions do you have for the draft CONOPS? Does the CONOPS provide useful information? Please include the relevant page number and paragraph/section.

7. Would you be interested in helping plan future cyber security events with PNWER's Center for Regional Disaster Resilience?

8. Would you like to be involved in the Center for Regional Disaster Resilience's Advisory Group? YES--NO

Optional/Required if interested in joining CRDR Advisory Group

Name:_____
Title:_____
Organization:_____ Email: _____

Thank you for your feedback. Please return this form to organizers as you leave.