Maritime Cyber Attack Scenario Discussion-Based Exercise Development Kit

Maritime Incident Preparedness and Response Discussion-Based Exercise Project

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

LSU
Stephenson Disaster Management Institute

June 2017

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is "*Maritime Cyber Attack Scenario Discussion-Based Exercise Development Kit*".

2. The information gathered in this kit is unclassified and is intended to have the widest distribution as possible among the Port and Maritime communities. This document should be shared with any facility and / or port that has a need to protect its informational and operational technology infrastructure.

3. The information contained in this document is the result of collaboration of many partners through the development of several cyber security discussion-based exercises. Contributors to this kit include the following agencies: U.S. Coast Guard Sector New York and Sector New Orleans, U.S. Coast Guard District 8, Louisiana State University Transformational Technologies and Cyber Research Center, U.S. Department of Homeland Security National Cyber Exercise and Planning Program, the Maritime and Port Security – Information Sharing and Analysis Organization, the Area Maritime Security Committee's for the Port of New York/New Jersey, Port of New Orleans and the Gulf of Mexico.

4. Principal Investigator for this project and Point of Contact for any additional information:

   Brant Mitchell
   Director
   Stephenson Disaster Management Institute
   Louisiana State University
   bmitch9@lsu.edu

CONTENTS

This material is based upon work supported by the U.S. Department of Homeland Security under Cooperative Agreement No. 2014-ST-061-ML0001.

PROJECT OVERVIEW

Background

The Maritime Security Center (MSC), a DHS Center of Excellence in Maritime and Port Security led by Stevens Institute of Technology, in conjunction with the Stephenson Disaster Management Institute (SDMI) at Louisiana State University has been working to develop scenarios and tabletop exercise resources to enhance the core capabilities and preparedness of port facilities and port operators to an array of hazards, including natural and man-made threats. It is the MSC's intent to extend these resources to the broad spectrum of port partners that comprise the maritime community, including public and private, local, state and Federal organizations. The MSC/SDMI tabletop exercise program builds upon other nationally recognized Executive Education Programs to provide support and resource materials for maritime and port stakeholders to develop and exercise their own tabletop and discussion-based activities.

Prior to the participation and development of any exercise content, staff from MSC and SDMI met with key stakeholders, to include the U.S. Coast Guard, Sector New York and Sector New Orleans, to discuss a range of scenarios that were critical to the ports. Through these dialogues, the two areas of concern that were most commonly identified involved active shooter, with emphasis on an event taking place at a cruise terminal, and cyber-based intrusions for nefarious purposes. Based on the requirement to develop exercises for these two emerging threats, the initial focus of this initiative has been geared towards developing content that will assist exercise design teams in developing realistic scenarios for active shooter and cybersecurity disruptions. As part of the process of developing content, scenarios and exercise design resources, the SDMI team worked directly with the Port of New Orleans, Port of New York/New Jersey, U.S. Coast Guard Sector New York and New Orleans, U.S. Coast Guard District 8, the DHS National Cyber Exercise and Planning Program, The Maritime and Port Security – Information Sharing and Analysis Organization (MPS-ISAO) and the Area Maritime Security Committee for the Gulf of Mexico to develop an active shooter exercise and multiple cyber-based exercises. Content from these exercises, as well as additional content, has been developed by an SDMI working group consisting of emergency managers, cyber experts, port officials, and Master Exercise Practitioners to provide a series of exercise scenarios to be used by ports and their tenants to test core capabilities related to active shooter and cyber threats.

The final year of this project has focused on integrating the lessons learned from the development and design of five separate exercises into the design and deployment of an "Exercise-in-a-Box" development kit to be leveraged by port facility affiliated exercise design teams. The purpose of the exercise development kits is to assist and enable port facilities and USCG Sectors to customize and conduct their own discussion-based exercises focused on

responding to active shooter and cyber-based threats. The complete series of exercise scenarios can be found on the MSC website at:

https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/education-training/tabletop-exercise-development-kits.

Exercise Development Kit - Overview

The Cyber Attack Discussion-based Exercise Development Kit is designed to provide an array of potential vulnerabilities to common assets and/or systems that can be exploited by a cyber attack. The exercise injects are not meant to tell a specific story but rather to provide a host of what appears to be non-related cyber events that have the potential to be a full-scale cyber attack directed at a specific port or the maritime industry as a whole. Based on the reach and complexity of a potential cyber attack throughout the entire maritime sector, the exercise development kit is designed to allow an exercise design team to integrate cyber attacks on key systems or assets that are commonly found in port facilities. The intent is to allow the team to introduce a variety of cyber-based injects that can negatively impact nearly any facility within a port. The injects are also designed to be layered in order to introduce attacks on multiple facilities or attacks throughout the entire port system. By developing injects for critical systems, the design team has the flexibility to create a wide variety of cyber attacks based on the goals and objectives of the exercise as well as meet the capabilities of specific facilities. In addition, the multiple injects allow for a wide array of sophistication of attacks based on the skill level of the exercise players.

The exercise scenarios are built around four modules. The first module is the "Threat Alert" module, and is designed to facilitate discussion on existing security postures and how participants would respond if there was a specific threat indicator that would raise awareness of a potential cyber attack. The second module is the "Initial Cyber Incident" module, in which the players are exposed to actual anomalies and disruption that could be attributed to a cyber attack. The purpose of the "Initial Cyber Incident" module is to initiate discussion on what protocols and incident response plans exist. In addition, determining whether or not the incident is significant enough to report to the Coast Guard is also meant to be part of the dialogue. Module three is the "Escalation" module, the cyber attacks are focused primarily on Industrial Control Systems in which secondary and tertiary order of effects could cause significant disruption to the maritime sector and/or the port. The fourth and final module is the "Post-Event" module, which is meant to allow the participants to discuss how a cyber attack on their facility may change their security posture and detection efforts moving forward. In addition, the opportunity to discuss forensics and attribution post event is also provided.

This development kit is meant to serve as a resource to help port/facility exercise planners create most aspects of a discussion-based exercise. This kit was designed according to guidelines established by the Homeland Security Exercise and Evaluation Program (HSEEP) and includes

scenarios that are intended to address and meet annual reporting requirements for organizations to exercise their Facility Security Plans.

Exercise Development Kit – Components/Resources

Each exercise development kit includes the following components:

1) **List of Potential Players** – Based on experiences with the exercises that were developed as part of this project, a list of potential players/participants is provided for consideration. This is not a complete list and should be tailored according to one's own relevant port/facility partners and operational environments. This list serves as a guide on potential agencies that may have an important capability / responsibility during a cyber attack. Suggested participants are listed by agency and not by individual agency components. It's important for the exercise planning team to recognize however, that recommended agencies may have more than one entity that should be at the table.

2) **Core Capability Alignment** – DHS/FEMA has published a list of 32 core capabilities. While all core capabilities may not be completely relevant to a cyber attack, there are several that are applicable. As part of the development kit, we are providing a list of core capabilities that can be aligned to a cyber related attack within the port system.

3) **Recommended Objectives** – For each of the relevant core capabilities, we have also identified potential / sample objectives that can be leveraged for the exercise. These objectives are intentionally written in a way that is generic and not specific to any particular participant or process being evaluated in an exercise. If the exercise design team identifies objectives that are relevant to their exercise, they can use as is or add more clarity and specificity to each of the relevant objectives.

4) **Scenario Builder (Injects)** – The scenario builder provides multiple injects for each of the four modules. The multiple injects allow the exercise design team to take different actions for a cyber attack while increasing the overall level of complexity and range of events. The injects can be used as they are currently written, or can be modified to suit an organization's unique needs. These injects are meant to serve as a starting point and provide a foundation on which to develop progressively complex scenarios.

5) **Facilitator Guide** – The exercise facilitator guide identifies a series of questions that can be utilized by a facilitator during a cyber attack discussion-based exercise. The list of questions is intended to drive discussion and dialogue among the exercise participants.

6) **Sample Exercise Outline** – To help the exercise design team construct a complete exercise from start to finish, a sample exercise outline that includes objectives

developed from core capabilities, injects, and facilitator questions is included. The sample exercise outline was developed using the information contained within this kit.

LIST OF POTENTIAL EXERCISE PLAYERS/PARTICIPANTS

This section contains a list of recommended participants and observers that should be considered when developing an invite list for the tabletop exercise. Ultimately, it is up to the organization's exercise design team to determine who should be a participant/observer. Some of these agencies should also be considered when developing the exercise design team. When warranted, clarification for each of the listed agencies is provided.

Participants

Port/Facility Administration: Port/Facility Administration should include members from the C-Suite (CEO, CIO, COO, CFO etc.), including Operations Personnel and Port Facility Security Officer (FSO).

Port Authority/Harbor Police

Port Partner Facilities/Organizations: Port Partner Facilities meeting the requirement to have an FSO should be considered to participate, together with other ancillary organizations. (i.e. second and third-party vendors.)

U.S. Coast Guard: Representatives from the local USCG Sector should be considered for inclusion in the exercise. Those members may include the Captain of the Port (or designee), Port Security Specialist, and uniformed member(s) from Contingency Planning and Response.

Local Homeland Security / Emergency Preparedness Office

Local Police Department

State Police / State Patrol: Consider including representatives from the local troop and headquarters.

State Homeland Security / Emergency Preparedness Office: Consider including representatives from Operations. Some states also have personnel dedicated to Intelligence Sharing and Critical Infrastructure within their offices.

State Fusion Center

Federal Bureau of Investigation – FBI field offices include Special Agents that are trained in responding to Cyber Security related events. There are also national assets at FBI HQs as well.

FBI Computer Crimes Task Force (members beyond the FBI): The FBI currently has 91 Computer Crime Task Forces across the United States. The teams consist of Federal, state and local members. Consider inviting members of the Task Force to participate or observe the exercise.

National Guard: Some states are now in the process of fielding National Guard Cyber Protection Teams. Participants should include someone from the state headquarters' Joint Directorate of Military Support to Civilian Authorities (JDOMS), as well as a representative from the HQ's Joint Directorate for Operations. Each state National Guard also has a Defense Cyber Operations Element (DCOE) that assist with the defense of the State's information technology network. A member from the DCOE should be considered to participate.

DHS Protective Services: The DHS Protective Services representatives serve as a conduit in relaying information on the status of affected federal critical infrastructure.

National Cybersecurity and Communications Integration Center (NCCIC): NCCIC provides 24x7 cyber situational awareness, incident response and management center for the Federal government. NCCIC deploys Hunt and Incident Response Teams (HIRT Teams) that serve as a response capability for the agency to assist critical infrastructure during cyber attack events. State-based NCCIC divisions also exist (i.e. NJCCIC) and maybe more appropriate to include in the exercise.

US-CERT (Cyber Emergency Response Team): Provides threat intelligence through alerts to the US public and private sector.

ICS-CERT: Provides threat intelligence specific to industrial control systems and the infrastructure sector.

Maritime & Port Security – Information Sharing and Analysis Organization (MPS-ISAO): Provides the maritime critical infrastructure with a trusted and secure public/private collaborative infrastructure and information sharing platform.

CORE CAPABILITY ALIGNMENT

The Homeland Security Exercise and Evaluation Program (HSEEP) calls for the identification of core capabilities to be exercised as a preliminary and essential part of the exercise design process. Conversations with port officials, the local USCG Sector, or port facility decision makers as to the current priorities/concerns in the port system, can help shape exercise objectives and the core capabilities to be exercised.

The following core capabilities have been identified as having the most applicability for a cyber attack involving a port facility / vessel. Prior to moving forward with the exercise design, the exercise design team should review the list of all 32 core capabilities, as part of the National Preparedness Goal, to determine if there are other core capabilities they may want to integrate into the design. To ensure the exercise focuses on specific capabilities, the exercise design team should select three or four of the core capabilities to be assessed in the exercise.

Relevant Core Capabilities for a Cyber Attack Exercise

Risk Management: Identify, assess, and prioritize risks to inform Protection activities and investments.

Intelligence and Information Sharing: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national homeland security by Federal, state, local and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among Federal, state, local, or private sector entities as appropriate.

Screening, Search and Detection: Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio-surveillance, sensor technologies, or physical investigation and intelligence.

Access Control and Identify Verification: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

Cybersecurity: Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Operational Coordination: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Situational Awareness: Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.

Forensics and Attribution: Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source, to include forensic analysis as well as attribution for an attack and for the preparation for an attack, in an effort to prevent initial or follow-on acts and/or swiftly develop counter-options.

Economic Recovery: Return economic and business activities (including food and agriculture) to a healthy state, and develop new business and employment opportunities that result in a sustainable and economically viable community.

RECOMMENDED OBJECTIVES

The following objectives are meant to serve as a guide for the exercise design team to consider in developing their own exercise objectives. The objectives below are not a complete list and can be modified and tailored to the exercise team's goals and to the unique nuances of the port/facility and players participating in the exercise. The objectives are intentionally written to be broad and non-specific to any one port or facility.

1) **Intelligence and Information Sharing:**

   Objective 1a: Validate that the Port/Facility has identified the personnel and procedures for conducting intelligence and information sharing of cyber threat and attack information with Federal, state, local, private sector, and international partners in order to share relevant, timely, and actionable information and analysis.

   Objective 1b: Ensure the Port/Facility possesses or has access to a mechanism to submit and receive cyber threat and attack related information and/or suspicious activity reports to law enforcement (i.e. NCCIC, Fusion Center, USCG Sector, FBI, local law enforcement).

   Objective 1c: Assess the ability of the Port/Facility to anticipate and identify emerging and/or imminent threats through the intelligence cycle.

   Objective 1d: Identify strengths, gaps, and needs in the intelligence and information-sharing environment of the Port System.

   Objective 1e: Assess the ability of the Incident Response Team to provide actionable information to the Port/Facility's information and analysis personnel during an active cyber-incident.

   Objective 1f: Assess the ability of Port/Facility to provide ongoing intelligence to their relevant Fusion Center or Information Sharing and Analysis Center (ISAC) or Organization (ISAO) during an active cyber incident response (i.e. LA-SAFE, MS-ISAC, MPS-ISAO).

   Objective 1g: Assess the ability of the state / local fusion center to disseminate intelligence throughout the Port System with emphasis on private sector facilities.

2) **Risk Management:**

   Objective 2a: Ensure that Port/Facility has and maintains a risk assessment process to identify and prioritize assets, systems, networks, and functions.

Objective 2b: Ensure that the Port/Facility's risk assessment defines cyber vulnerabilities as well as the likelihood and the potential consequences of that vulnerability to be exploited, are considered for each asset, system, network, or function.

Objective 2c: Determine if the current Facility Security Plan (FSP) assesses vulnerabilities of physical security technologies/systems in the Port/Facility's overall risk assessment. (i.e. Cameras, radios, access control)

Objective 2d: Determine if the current FSP and Cyber Security Plan nest well together and are sufficient to prepare for and respond to a cyber event.

Objective 2e: Identify areas of improvement for the emergency management / risk management program.

Objective 2f: Establish and identify the current operating picture and risk management strategy pertaining to the Port/Facility's cyber security program.

3) **Screening, Search and Detection:**

Objective 3a: Identify if the Port/Facility utilizes network-based and host-based intrusion detection tools.

Objective 3b: Determine if current intrusion detection tools monitor both inbound and outbound communications for unusual or unauthorized activities.

Objective 3c: Determine if the Port/Facility maintains a repository of all intrusion detection logs in a central logging facility to allow for correlation and analysis.

Objective 3d: Examine the Port/Facility's capability to support near-real-time analysis of events in support of detecting cyber attacks.

Objective 3e: Identify the actions of the Port/Facility upon detection of a cyber breach/attack.

4) **Access Control and Identify Verification:**

Objective 4a: Determine if the Port/Facility's current implementation of security mechanisms restrict access to all or specific systems according to defined roles, and follow the principle of least privilege.

Objective 4b: Determine if current information systems restrict access to privileged functions and security relevant information to specific authorized personnel.

Objective 4c: Determine if the Port/Facility adequately authenticates the identifies of users as a prerequisite to allowing access to information systems and services.

5) Cybersecurity:

Objective 5a: Identify if the Port/Facility implements risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.

Objective 5b: Assess if the Port/Facility implements and maintains procedures to detect malicious activity to conduct technical and investigative-based countermeasures, mitigations, and operations against malicious actors to counter existing and emerging cyber-based threats, consistent with established protocols. (i.e., NIST, ABS)

Objective 5c: Ensure that the Port/Facility implements controls to mitigate the vulnerabilities identified during the risk management framework.

Objective 5d: Assess the effectiveness of the Port/Facility's current cyber security systems to protect itself from cyber attacks.

Objective 5e: Determine if current cyber security awareness and training plans adequately reduce the Port/Facility's risk from a cyber attack.

6) Operational Coordination:

Objective 6a: Examine the operational coordination requirements between the local, state, and Federal agencies in response to an active cyber attack.

Objective 6b: Enhance the ability of the Port/Facility leaders and decision makers to respond to a major cyber attack.

Objective 6c: Examine the limits of mutual aid, with the intent to determine the capabilities of the Port/Facility to respond to a cyber event absent of substantial and immediate assistance.

Objective 6d: Develop a common understanding of key homeland security cyber policies, emergency management cyber strategies, authorities, plans, and organizational structure.

Objective 6e: Identify gaps and needs in the command and control structure of the Port/Facility's cyber incident response.

7) **Situational Awareness:**

Objective 7a: Determine the effectiveness of port officials / port facilities to share information and provide situational awareness to local first responders and cyber response teams.

Objective 7b: Determine the effectiveness of port officials / cyber incident responders to develop situational awareness of a cyber attack at a port facility.

Objective 7c: Determine the effectiveness of port officials / local cyber response teams to monitor social media and the dark web to enhance situational awareness of an escalating event at a port facility.

Objective 7d: Determine if the Port/Facility's network intrusion detection systems are sufficient to alert the port system of an immediate cyber attack.

8) **Forensics and Attribution:**

Objective 8a: Determine the effectiveness of port officials to identify compromised and impacted systems across the port's network.

Objective 8b: Determine the effectiveness of port officials / local cyber response teams' ability to analyze logs and impacted systems in order to identify tactics, techniques and procedures utilized by the cyber attackers to comprise systems.

Objective 8c: Determine the effectiveness of port officials / local cyber response teams' ability to balance the needs of evidence preservation against the requirement to restore systems back to a good state.

9) **Economic Recovery:**

Objective 9a: Identify potential fallouts from a cyber attack on a Port/Facility and the sequence of actions to mitigate impacts and ensure the Port/Facility is able to fully recover economically.

Objective 9b: Determine whether or not the Port/Facility's Continuity of Operations Plan is adequate in dealing with a cyber attack at a port facility.

Objective 9c: Assess the Port/Facility's recovery plan to determine if it is sufficient in addressing a potential fallout from a cyber attack.

Objective 9d: Determine how the Port/Facility would implement immediate short term recovery procedures in response to a cyber incident

SCENARIO BUILDER AND INJECTS

The cyber scenarios below are designed around four modules: Module 1 – Threat Alert; Module 2 – Initial Cyber Incident; Module 3 – Incident Escalation; Module 4 – Post-Incident. For each module, multiple injects are provided to allow the exercise design team to develop an exercise that meets the team's specific goals and objectives. The exercise design team can pick and choose the injects in any combination that ultimately facilitates the assessment of objectives for their specific Port/Facility exercise. When deciding on which injects to use, exercise designers are encouraged to change elements of the injects to make them more applicable to the participating Port/Facilities.

The Cyber-Attack Discussion-based Exercise Development Kit is designed to provide a hypothetical array of potential vulnerabilities to common assets and/or systems that can be exploited by a cyber attack. The injects are not meant to tell a specific story but rather to provide a host of what appears to be non-related cyber events that have the potential to escalate to a full-scale cyber attack directed at a specific port, or to the maritime industry as a whole. Based on the breadth and complexity of a potential cyber attack throughout the entire maritime sector, the exercise development kit allows an exercise design team to integrate cyber attacks on key systems or assets that are commonly found in port facilities. The intent is to allow the team to introduce a variety of cyber-based injects that can negatively impact nearly any facility within a port. The injects are also designed to be layered in order to introduce attacks on multiple facilities or attacks throughout the entire port system. By developing injects for critical systems, the design team has the flexibility to create a wide variety of cyber attacks based on the goals and objectives of the exercise as well as meet the capabilities of specific facilities. In addition, the multiple injects allow for a wide array of sophistication of attacks according to the skill level of the exercise participants.

The first module in the exercise sequence is the "Threat Alert" module, and is designed to facilitate discussion on existing security postures and how participants would respond if there was a specific threat indicator that would raise awareness of a potential cyber attack. The second module is the "Initial Cyber Incident" module, in which the participants/players are exposed to anomalies and disruptions that could be attributed to a cyber attack. The purpose of the "Initial Cyber Incident" module is to initiate discussion on what protocols and incident response plans exist. In addition, determining whether or not the incident is significant enough to report to the Coast Guard is also meant to be part of the dialogue. Module three is the "Escalation" module, the cyber attacks are focused primarily on Industrial Control Systems (ICS) in which secondary and tertiary order of affects could cause significant disruption to the maritime sector and/or the port. The final module is the "Post-Event" module, which is intended to allow the participants to discuss how a cyber attack on their facility may change their security posture and detection efforts moving forward. In addition, the opportunity to discuss forensics and attribution post event is also provided.

Module 1 – Threat Awareness

The first module, Threat Awareness, is designed to explore the current security posture and risk management framework currently employed within a port facilities cyber infrastructure. The intent of the first inject is to raise awareness that the potential threat of a cyber attack exists and whether or not the port as a whole or individual facilities within the port will alter their current security posture. This module is also designed to assess the ability of Federal, state, and local intelligence gathering assets to share information across the port system. Injects 1a and 1b are general technical alerts from US-CERT and ICS-CERT providing warning of potential cyber threats. Inject 1c and 1d are based on proof of concept reports disseminated by the Maritime & Port Security – Information Sharing and Analysis Organization (MPS-ISAO). Finally injects 1e and 1f are designed for more sophisticated IT departments doing proactive monitoring of their networks and notice anomalies that indicate a breach may have occurred.

Module 1 (Threat Alert / Identification) – Core Capability Alignment:

Information and Intelligence Sharing

Risk Management

Module 1 (Threat Alert / Identification) Injects:

Inject 1a: US-CERT issues a Technical Alert (TA) providing warning of a new widespread ransomware campaign that exploits a windows vulnerability. A primary infection vector appears to be through a phishing campaign.

Inject 1b: ICS-CERT issues an Alert that is reporting a common power management system used throughout the maritime industry, that is susceptible to being managed remotely.

Inject 1c: The Maritime Port Security – Information Sharing and Analysis Organization (MPS-ISAO) distributes a proof of concept from a security firm that a suspected cyber attack that negatively impacted a shallow water vessel. The report indicates the event can be a potential maritime sector-wide threat.

Inject 1d: The Maritime Port Security – Information Sharing and Analysis Organization (MPS-ISAO) distributes a proof of concept from a prominent university that a common Programmatic Logic Controller are susceptible to a cyber attack.

Inject 1e: IT personnel monitoring the company's intrusion detection system notice a port scan has been conducted against their network by a source identified in a technical alert issued by US-CERT.

Inject 1f: The IT department is reporting that internal machines are communicating with external IP addresses on a regular and routine basis, including to an IP address that has been identified as a hostile actor by a technical alert issued by US-CERT.

Module 2 – Initial Cyber Incident

The second module, Pre-Incident / Incident, provides varying levels of complexity and information available to the participants. The goal of Inject 2 is to assess the ability of port facilities to determine initial responses to a suspected cyber attack. The injects are based on vulnerabilities being exploited by an asset/system. In using the injects to design the module, the exercise design team should consider who the participants will be and what systems they have that may be vulnerable to a cyber attack. For these injects the threat actors and motives are not necessary to move the dialogue forward. Instead the purpose is to initiate discussion on determining what the initial actions by the exercise players will be and whether or not the attack would rise to the level of being reported to the U.S. Coast Guard or the NCCIC. In order to simulate multiple attacks and to engage as many players as possible, the module should include as many of the seventeen injects as possible to develop the potential that there is the beginning of a port-wide attack and to engage multiple participants.

Module 2 (Initial Cyber Incident) – Core Capability Alignment:

Screening, Search and Detection

Access Control and Identify Verification

Cybersecurity

Module 2 (Initial Cyber Incident) Injects:

Inject 2a (Physical Security): The Facility Security Officer (FSO) receives a report that all security cameras throughout the facility have gone down.

Inject 2b (Physical Security): The automated gates that provide access into the facility have all moved to the open position and appear to be offline, and not responding to digital control system commands to go back to the closed position. Multiple unguarded entry points are providing access to the facility.

Inject 2c (Physical Security): The access control database used to verify entry into the facility has gone offline. Container trucks along with cars containing facility personnel are beginning to create a backlog along the port's/facility's access road.

Inject 2d (Physical Security): Personnel at the security gate allowing access to the facility are reporting that several employees for the company no longer appear in the access control database even though they are still employed with the company. HR reports that the employees are still in good standing with the company.

Inject 2e (Inventory Systems): The company's product inventory system is providing inconsistent data. The operator is reporting inconsistencies with known on hand quantities of product being different than what is reported in the inventory control system.

Inject 2f (Inventory Systems): While entering data into the company's inventory system on a company terminal, the inventory software suddenly disappears and a dialogue box appears on the screen with the notice that "This system's files have been encrypted". The dialogue box also provides instructions on how to obtain a private key in order to decrypt the data. The dialogue also instructs the user that the private key will cost 3,000 U.S. Dollars and will be destroyed in 96 hours if not purchased before that time.

Inject 2g (Programmable Logic Controller): A vessel about to begin its product transfer to the onshore facility reports a failure of the ship's Industrial Control System that controls the flow of product to and from the vessel. The Captain of the vessel notifies the Facility Security Officer (FSO) that their Chief Engineer has found a USB inserted into a USB port on the vessel's Industrial Control System that controls the flow of product to and from the vessel.

I**nject 2h (Industrial Control System)**: – An operator notices that the mouse on their Human Management Interface (HMI) is moving on its own.

Inject 2i (Navigational Systems): Several cranes at a container facility that were in the process of off-loading containers from a vessel all of a sudden experience disruptions in their operational capability. An initial investigation looks like all cranes are experiencing a GPS signal disruption which is preventing the cranes from determining its exact location.

Inject 2j (Navigational System): At ___Date/Time_____ the Facility Security Officer (FSO) receives a report from the vessel's agent discharging at the dock that they were unable to depart at the conclusion of the transfer due to a failed navigational system on the vessel's bridge. 30 minutes later, the Captain of the vessel calls the FSO to state that one of their officers located a USB inserted into a USB port that has access to the Navigational System. Another vessel is scheduled to dock shortly after the scheduled departure of the vessel currently attempting to conclude their transfer.

Inject 2k (Billing Systems): The CFO receives a report from the facility's Chief Information Security Officer (CISO) that their billing system, to include their client list and pricing structure, has been compromised and a large data transfer to an anonymized IP address has occurred.

Inject 2l (Billing System): An accountant preparing a billing sheet for a client notices some irregularities in the costs for services. The accountant notices that prepopulated costing structures have been changed. After reporting this to the IT department and looking into

the billing structure, it appears that the accounting system has been compromised and the facilities pricing schedule has been maliciously adjusted.

Inject 2m (Billing System): While entering data into the company's billing system on a company terminal, the accounting software suddenly disappears and a dialogue box appears on the screen with the notice that "This system's files have been encrypted". The dialogue box also provides instructions on how to obtain a private key in order to decrypt the data. The dialogue also instructs the user that the private key will cost 3,000 U.S. Dollars and will be destroyed in 96 hours if not purchased before that time.

Inject 2n (Accounting System): The CFO/Accountant receives an email that at first appears to be from the president of the company, directing them to transfer money to an account for services rendered by a provider. The president has asked him to do this before so he doesn't think twice about making the transfer. After the transfer has been made, the IT department notices that the president's email account has been compromised.

Inject 2o (IT Infrastructure): The company's webmaster reports that the company's webserver has been compromised and the company's public website has been defaced with environmental propaganda (alternate scenario – ISIS propaganda).

Inject 2p (IT Infrastructure): The Chief Information Security Officer (or IT personnel for smaller companies) is reporting that there has been a failure of their domain controller, and that it has crashed due to an unknown cyber attack. All email and network file share for the company is currently impacted and not available for company personnel.

Inject 2q (IT Infrastructure): Early in the morning, an email that appears to be from Human Resources about a change to the company's retirement plans was sent to all employee emails. The email instructs employees to click on an attachment to get more information. Approximately 7% of the employees click on the email causing all of their machines to get encrypted.

Module 3 – Incident Escalation

The Incident Escalation module provides the exercise participants the opportunity to discuss how they would respond to a cyber attack that has the potential to cause environmental damage and disrupt maritime transportation. This module is designed to explore the operational coordination and operational communication issues between the facility and responding Coast Guard officials. Each inject offers an additional element of complexity to the injects provided in Module 2 with significantly greater secondary and tertiary effects from the attack. Like Module 2, the exercise design team should use as many injects they feel are necessary to imply that there is a port-wide cyber attack.

Module 3 (Cyber Incident Escalation) – Core Capability Alignment:

Cybersecurity

Operational Coordination

Situational Awareness

Module 3 (Cyber Incident Escalation) – Injects:

Inject 3a: (Inventory Systems): IT personnel at a container facility have identified that the Container Shipment Database appears to have been accessed and manipulated. The database has had approximately 300 containers deleted.

Inject 3b (Industrial Control Systems): Early this year a spear phishing campaign was launched against energy-related organizations across the maritime sector, to include third party contractors. The third party contractor's staff provides services to multiple facilities across the port and as a result have left dormant malware on several Industrial Control Systems that control power generation. An anomaly is noticed by a pipeline hub operator in its enterprise network traffic and they begin investigating. Initial analysis of the malware that was identified by an outside cyber expert indicates that the malware is targeting Operational Technology (OT) systems.

Inject 3c (Industrial Control Systems): After experiencing some irregularities earlier in the transfer process, sounding and pressure gages are brought back online following a hard restart. While monitoring the transfer, the operator of the Industrial Control System (ICS) loses total control of the transfer and pressure readings suddenly spike. Shortly after the transfer pipeline bursts and multiple alarms inundate the ICS, including both low and high pressure alarms. Additionally, low and high sounding alarms activate the facility's storage tanks.

Inject 3d (Industrial Control Systems): A bulk transfer storage operator observes a disruption to its power management system. Malware overrides safety/alarms and computers to show regular operations while the power system is being disrupted.

Inject 3e (Industrial Control Systems): A mobile offshore drilling platform experiences a disruption to its power management system. The disruption poses the possibility of impacting its dynamic positioning, which could result in a drift-off situation and emergency disconnect.

Inject 3f (Industrial Control Systems): ICS operators are reporting that their Human Management Interface (HMI) controls are being manipulated by a remote user. Operators in the plant are reporting that product transfers are beginning to occur while the HMI is showing that all transfer systems are not currently in use.

Inject 3g (Navigational Systems): – Several cranes at a container facility that were in the process of off-loading containers from a vessel all of a sudden experience disruptions in their operational capability. Initial exploration looks like all cranes are experiencing a GPS signal disruption, which is preventing the cranes from determining its exact location.

Inject 3h (IT Infrastructure): Following a spear phishing attack earlier in the day, security is reporting that entrance and exit gates are having issues with the access control database. The loss of the access control database is resulting in significant traffic issues that are beginning to disrupt other port operations and facilities.

Module 4 – Post Incident

The purpose of Module 4 – Post Incident, is to bring a conclusion to the immediate threat and facilitate discussion about the immediate and long-term recovery from a cyber attack. In addition, it provides an opportunity for those facilities with mature IT staffs to discuss forensics and attribution. The injects are similar to one another but vary only in regards to the availability or lack thereof of data backups.

Module 4 (Post Incident) – Core Capability Alignment:

Forensics and Attribution

Economic Recovery

Module 4 (Post Incident) – Injects:

Inject 4a: The cyber incident response team has identified several network connected computers that have been infected with a ransomware variant. The team has physically severed the network connections of all the devices and have determined that the ransomware threat has been contained but not eradicated.

Inject 4b: The cyber incident response team has identified several network connected computers that have been infected with a ransomware variant. The team has physically severed the network connections of all the devices, formatted all the devices and performed complete reinstalls of all operating systems. The team has contained and eradicated the ransomware. System backups from the previous day were available for all impacted systems resulting in the loss of one day's worth of data.

Inject 4c: The cyber incident response team has identified several network connected computers that have been infected with a ransomware variant. The team has physically severed the network connections of all the devices and pulled forensic images of the impacted systems for further analysis and to share with law enforcement. Complete

reinstalls of the impacted machines was done; however, there are no up-to-date system backups available, which has resulted in the loss of 6 months of data.

Inject 4d: The cyber incident response team has identified several network connected computers that have been infected with a ransomware variant. These infected machines include the port / facility's domain controller and primary file share. System backups from the previous day were available for all impacted systems resulting in the loss of one day's worth of data.

Inject 4e: The cyber incident response team has identified several network connected computers that have been infected with a ransomware variant. These infected machines include an engineering workstation used within the Industrial Control System network. The team has physically severed the network connections of all the devices and pulled forensic images of the impacted systems for further analysis and to share with law enforcement.

Inject 4f: The cyber incident response team has identified several network connected computers that have been compromised by a remote access tool and data stealing trojan. These infected machines contained data sensitive information to the port / facility. The team confirms that the data was transferred to an anonymized IP address. The team has physically severed the network connections of all the devices and pulled forensic images of the impacted systems for further analysis and to share with law enforcement.

FACILITATOR GUIDE

One of the most important aspects of any discussion-based exercise is the development of a comprehensive script for the facilitator. This part of the development kit is designed to provide a framework in which any exercise design team can establish an initial foundation of relevant questions for a facilitator to ask during the actual delivery of the exercise. The questions are organized by module and by core capability. The Facilitator Guide is not a complete list of all relevant questions. These questions are general, and are meant to apply to any participant of a facility. When designing the final bank of questions, the exercise design team should include questions that are based on actual security policies and procedures, including the Facility Security Plan and other relevant sources that are specific to the port community. Once the specific core capabilities for an exercise are settled upon, the exercise design team should review some of the questions from the other core capabilities as they may be loosely related to other capabilities not selected for the exercise.

Questions for Inject 1 – Threat Alert

Core Capability: Information and Intelligence Sharing

1. How does threat information get disseminated to the Port Enterprise System?

2. From a regional perspective, how does the intelligence process work – Federal, state, and local flow of information? Is there too much reliance on the Federal government to take the lead on Intelligence?

3. Describe the Intelligence Fusion system in your state and your city and how information is shared with the port.

4. What process is used to collect, fuse, analyze, and disseminate intelligence and information products? What is the status of intelligence and information fusion efforts? Is it meeting your expectations?

5. Should all disciplines be involved? How are public health and other agencies incorporated into the intelligence collection, analysis/fusion, dissemination, and feedback process? Are there any policy or operational considerations?

6. How should regional entities be involved in intelligence sharing/collaboration?

7. What role does / should the private sector play in intelligence strategies? Are private sector entities within the port system getting access to information? How is it disseminated?

8. Are there any issues regarding legal authorities / statutory limitations to gather intelligence and share it with law enforcement – i.e. open meeting/disclosure laws, etc.?

9. Do you expect information and intelligence to be shared regionally?

10. Who should drive or determine the end products of the fusion process? What do elected officials expect as end products for their consumption?

11. Are you currently aware of the Alerts provided by ICS-CERT and US-CERT? Are any actions ever taken once these alerts are received? Are they shared?

12. Is there any broad based cyber related Alert that would cause the Captain of the Port to raise the MARSEC level?

13. What controls are currently in place for cyber assets when the MARSEC level is increased? Are the controls all based on physical security?

14. For conducting intelligence and information sharing regarding cyber threats? Does the Port/Facility have a procedure for receiving, analyzing and integrating cyber threat information from open or closed threat intelligence sources to protect from known or eminent cyber attacks?

15. Does the Port/Facility have a procedure for sharing their specific cyber threat / cyber attack information to the DHS National Cybersecurity and Communications Center (NCCIC), State Fusion Center, a representative Information Sharing Analysis Center or Organization (ISAC /ISAO)?

16. Does the Port/Facility have an automated mechanism for submitting and receiving cyber threat intelligence information to Fusion center, FBI, local law enforcement, etc?

17. Does the Port/Facility have an automated mechanism for integrating cyber threat data into their organizational protective informational technology (IT)? (i.e. Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) and Cyber Observable eXpression (CybOX))

18. Does the Port/Facility incorporate open/closed threat information into their protective technologies to prevent emerging and/or imminent threats?

19. Does the Port/Facility have a network baseline of what normal traffic for the network is? Does the Port/Facility monitor their network traffic for anomalies or suspicious activity? Identify strengths, gaps, and needs in the intelligence and information-sharing environment of the Port System.

20. What is the Port/Facility's communication plan between its Information and Sharing personnel and its internal or contracted incident response teams during an incident?

21. What is the communication strategy between the Port/Facility and their local law enforcement or Fusion Center, ISAC or ISAO during an active cyber event?

22. What is the communication strategy between the private Port/Facility and their local law enforcement or Fusion Center?

Core Capability: Risk Management

1. Are employees trained on how to respond to a suspected spear phishing attempt?

2. Does your facility have a cyber hygiene training program for your employees?

3. How often does your facility conduct risk assessments and what is the process for conducting the assessment?

4. How do you prioritize your risk? Where does cyber fall on this list?

5. Based on recent news events, is your threat for cyber where it needs to be?

6. At this time, what resources are made available for employees from a training and response perspective?

7. Has your facility completed a cyber vulnerability assessment? Have business functions been aligned with cyber related controls?

8. What are the greatest threats to the local port community?

9. Does your facility have safeguards against an insider threat? How about corporate espionage?

10. How valuable is your client list? What about your costing schedule? Do they need to be safeguarded?

11. How is the Federal government organized to identify threat? Is it meeting expectations? Are you aware of the resources that DHS provides to assist with cyber infrastructure?

12. Do you conduct routine risk assessments? Does your risk assessment process include the identification and prioritization of technology assets to include all business related data, transactions, and telecommunications? (i.e. Information Technology (IT) and Operational Technology (OT) equipment)? In your risk assessment, are your technology assets prioritized by impact if stolen, changed without authorization, or made unavailable?

13. Does your risk assessment consider all known vulnerabilities to those identified technical assets? Do you consider the likelihood of these vulnerabilities being discovered and exploited? Do you consider the potential consequences of these assets being stolen, changed, or made unavailable?

14. Does your risk assessment consider the loss of physical security technologies such as cameras, access control gates, communication tools or other technology used by physical security personnel?

15. Do your cyber security planners and facility security planners communicate common risks, mitigations, and security measures?

Questions for Inject 2 – Initial Cyber Incident

Core Capability: Screening, Search and Detection

1. What systems does the Port / Facility currently use to provide network and host-based intrusion detection?

2. Do those tools have the capability to provide intrusion prevention (i.e., can they alert for both an attack and block an attack)?

3. Does the Port/Facility deploy intrusion detection tools both within the network and at the network's perimeter?

4. Are these systems rule or anomaly-based?

5. If rule based, how often are the rules updated? If anomaly based, how long did the tool run in baseline mode?

6. Does the Port/Facility utilize a centralized syslog or security information and event management (SIEM) server?

7. If so, does the Port / Facility use an analytical tool to review those logs?

Core Capability: Access Control and Identify Verification

1. What are your current security protective measures that rely on IT or OT systems?

2. What are normal day to day security levels?

3. At what point is the security level raised? Who makes this decision? Who is the decision shared with internally and externally?

4. Is the Coast Guard notified? If so, when?

5. How do your employees get in your facility? Do you have an access control database that requires authentication such as an ID? Do you have manual processes in the event the digital system is offline?

6. If you have any type of disruptions to your access control is any of this information shared with other port partners? Is it shared with the Coast Guard?

7. What are your protocols if the camera system goes down?

8. What are your protocols if the gate system doesn't function properly? If the gates are locked in an open mode, do you have the resources to provide personnel to augment until they are brought back online?

9. Would the protocol for a physical security incident differ from a cyber incident with regards to a physical IT/OT asset being off line?

10. Are physical security and operational systems protected equally?

11. Are IT personnel notified that cameras are inoperable and the gates remain open?

12. With the loss of one physical control system, would you change your security level / posture? What about two systems? What about your access control database?

13. Has the Port / Facility ever performed a vulnerability assessment or penetration test to assess the effectiveness of current systems ability to restrict access according to defined roles?

14. Has the Port / Facility ever performed a vulnerability assessment designed to test that access to privileged functions is restricted to authorized personnel?

15. Based on the available information, would the Captain of the Port consider raising the MARSEC Level?

Core Capability: Cybersecurity

1. If an Industrial Control System (ICS) appears compromised and sounding / pressure readings were down, would you notify the Coast Guard? Would you notify adjacent facilities?

2. Who would you contact internally and externally?

3. With a compromised ICS, who / what would be impacted?

4. What potential hazards are created with the systems down?

5. Would there be a potential for a spill? An explosion?

6. How would it impact other processes and/or operations in the facility?

7. Would IT staff be notified of a suspicious email?

8. Would all phishing attempts hit the end points? Was it blocked?

9. What domain did they originate from?

10. Can you block a specific domain?

11. Who would normally ID, verify and block domains within the Port/Facility?

12. Has this happened before?

13. Has anyone in your organization had to deal with ransomware?

14. Does IT send out notifications and alerts regarding suspicious emails?

15. Were there any A/V alerts sent?

16. Does the Port / Facility have a risk based cyber security plan? If so, does the plan tie back to the regulations that the Port / Facility follows?

17. What procedures does the Port / Facility have in place to detect unauthorized network activity? How often are these procedures updated?

18. Are these procedures tied to a specific technology or are they broad-based?

19. Has the Port / Facility ever performed a vulnerability assessment or penetration test to assess the effectiveness of current cyber security systems? If so, did the test target users to determine the effectiveness of current cyber security and awareness training?

20. Based on the available information, would the Captain of the Port consider raising the MARSEC Level?

Core Capability: Operational Coordination

1. What is the current protocol in responding to a cyber attack at your facility? Are personnel properly trained to respond?

2. Who would be notified? How would they be notified?

3. Would your current staff be able to respond to a major breach? Would they be able to regain control of an affected ICS? Could they manually terminate the ICS process?

4. If you were unable to respond internally with your existing resources, who would you reach out to?

5. What is the Coast Guard's role in an event like this?

6. Are there existing relationships with state and local cyber resources?

7. If the cyber event is believed to be a terrorism event instead of a random cyber incident, how does that change the response? Does it change who is in charge of the response? Who has ultimate authority?

8. What resources does the Coast Guard have that they could influence the outcome of a cyber attack?

9. Has the Port / Facility ever participated in a cyber exercise with local, state and Federal partners?

10. Does the Port / Facility have a clear understanding of what to share with local, state and Federal partners as it relates to cyber?

11. Does the Port / Facility understand how shared information is handled by local, state and Federal partners?

12. Is the Port / Facility aware of existing local, state and Federal cyber resources that can be called upon to assist in the event of a cyber incident?

13. Based on the available information, would the Captain of the Port consider raising the MARSEC Level?

Questions for Inject 3 – Incident Escalation

Core Capability: Situational Awareness

1. How does the IT staff relay intelligence information to external stakeholders? To the Coast Guard?

2. How is the information being distributed to responding agencies?

3. Who would be responsible for painting the big picture? Does the Coast Guard have cyber trained personnel that can connect the dots?

4. What resources are available to help do that?

5. Does the Port / Facility routinely share information with local law enforcement and/or the fusion center?

6. If so, does this information include indicators of compromise (IOC), which are used to identify cyber attacks?

7. Does the Port / Facility know who to share IOCs with at the Federal, state and local levels?

8. Does the Port / Facility's information technology and/or cyber security personnel share network situational awareness derived from internal systems with other groups within the port or facility?

9. Would the Port / Facility's management be aware of a small to medium sized cyber attack that was handled internally?

10. Does the Port / Facility employ personnel to monitor social media and the dark web to identify potential threats?

11. Has the Port / Facility ever performed a network vulnerability assessment against web facing systems?

12. If so, was the assessment used to identify the effectiveness of current intrusion detection and/or prevention systems?

13. With this additional information, would the Captain of the Port consider raising the MARSEC Level?

Questions for Inject 4 – Post Incident

Core Capability: Risk Management

1. Having gone through a cyber related event, how does this impact your existing threat assessment?

2. Does this event change the way you prioritize your risk?

3. Based on this scenario, do you believe your threat for a cyber attack is where it needs to be?

Core Capability: Forensics and Attribution

1. What is the process for moving from response to recovery and standing down deployed measures?

2. Does the Port / Facility maintain a cyber incident response plan? If so, how often is it tested?

3. Does the plan identify key personnel to act in a cyber incident response role during an event?

4. Does the Port / Facility provide ongoing training for identified cyber incident response personnel?

5. Are any members of the incident response team certified as cyber incident handlers? Does the port have personnel trained in digital forensics?

6. If not, does the Port / Facility have a relationship with local law enforcement to perform that role?

7. Does the Port / Facility have an MOU or understanding in place with law enforcement in order to maximize both the preservation of evidence and the facilities requirement for a quick restoration?

Core Capability: Economic Recovery

1. Does the Port / Facility currently have a Cyber Insurance / Data Breach Insurance policy? If so, to what extent is the facility covered?

2. Does the policy cover insider threats?

3. What about cyber incidents caused by negligence?

4. Has the Port / Facility performed a critical asset identification process for networked systems and data?

5. Does the Port / Facility utilize a data classification guideline based off of that process?

6. If so, has the Port / Facility identified its “crown jewels”?

7. Has the Port / Facility ever tested the Continuity of Operations Plan as the result of an exercised cyber attack?

SAMPLE EXERCISE OUTLINE

Cybersecurity Discussion-Based Exercise

Developed by the Stephenson Disaster Management Institute at
Louisiana State University and the Maritime Security Center, Stevens Institute of Technology, New Jersey

"Identification of and Response to a Deliberate Cyber Attack"

Port of _____
Date
8:30 a.m. – 12:00 p.m.

Discussion Outline and Key Questions

Preface to the Discussion Outline: The Discussion Outline was developed as a tool to facilitate dialogue among the exercise participants and serve as a resource for follow-on exercises and future training opportunities. The list of questions and observations throughout the outline are intended to aid the exercise participants, and to serve as topics for consideration and conversation in exploring additional issues that may arise as the result of a cyber attack.

9:00 a.m.

Welcoming and Opening Remarks

Exercise Director

Program Purpose

The Maritime Security Center a DHS Center of Excellence in Maritime and Port Security in conjunction with SDMI is working to develop scenarios and tabletop exercise resources to enhance the core capabilities and preparedness of port facilities and port operators to an array of hazards, including natural and man-made threats. It is our intent to extend these resources to the broad spectrum of port partners that comprise the maritime community, including public and private, local, state and Federal organizations. The MSC/SDMI tabletop exercise program builds upon other nationally recognized Executive Education Programs to provide support and resource materials for maritime and port stakeholders to develop and exercise their own tabletop and discussion-based activities.

Agenda Review

- Under the Agenda Tab in participants handouts

Event Format

- Interactive roundtable discussion.
- Written Injects will be used to help frame issues.
- We want to explore unique emergency management challenges and issues at the Federal, state and local level. Particularly we want to understand the coordination issues between responding agencies and avoid tactical details.
- It is OK to debate current policies and each other.
- Primary focus will be on intergovernmental and private sector challenges as well as some of the unique response and recovery elements in a cyber scenario.
- Introductions

Introduction of the Exercise Participants

9:10 a.m.

Event Objectives and Key Questions

Event Facilitator

Exercise Objectives:

Core Capability: **Intelligence and Information Sharing**

Objective 1: Identify strengths, gaps, and needs in the intelligence and information-sharing environment of the Port System.

Core Capability: **Risk Management**

Objective 2: Determine if the current Facility Security Plan (FSP) assesses vulnerabilities of physical security technologies/systems in the Port/Facility's overall risk assessment. (i.e. Cameras, radios, access control)

Core Capability: **Cybersecurity**

Objective 3: Identify if the Port/Facility implements risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.

Core Capability: **Situational Awareness**

Objective 4: Determine the effectiveness of port officials / port facilities to share information and provide situational awareness to local first responders and cyber response teams.

9:20 a.m.

Opening Conversation

What are the priority risks and threats as perceived by the Port leadership?

What are the major consequences of a targeted and deliberate cyber attack event that keeps you up at night?

9:30 a.m.

Core Capability Focus Area: Intelligence Fusion and Information Sharing

INJECT 1a - US-CERT issues a Technical Alert (TA) providing warning of a new widespread ransomware campaign that exploits a windows vulnerability. A primary infection vector appears to be through a phishing campaign.

INJECT 1b - The Maritime Port Security – Information Sharing and Analysis Organization (MPS-ISAO) distributes a proof of concept from a security firm that a suspected cyber attack that negatively impacted a shallow water vessel. The report indicates the event can be a potential maritime sector-wide threat.

Facilitator Questions for Inject 1 (Emphasis on Intelligence and Information Sharing)

1. How does threat information get disseminated to the Port Enterprise System?

2. From a regional perspective, how does the intelligence process work – Federal, state, and local flow of information? Is there too much reliance on the Federal government to take the lead on Intelligence?

3. Describe the Intelligence Fusion system in your state and your city and how information is shared with the port.

4. What process is used to collect, fuse, analyze, and disseminate intelligence and information products? What is the status of intelligence and information fusion efforts? Is it meeting your expectations?

5. How should regional entities be involved in intelligence sharing/collaboration?

6. What role does / should the private sector play in intelligence strategies? Are private sector entities within the port system getting access to information? How is it disseminated?

7. Are there any issues regarding legal authorities / statutory limitations to gather intelligence and share it with law enforcement – i.e. open meeting/disclosure laws, etc.?

8. Are you currently aware of the Alerts provided by ICS-CERT and US-CERT? Are any actions ever taken once these alerts are received? Are they shared?

9. Is there any broad based cyber related Alert that would cause the Captain of the Port to raise the MARSEC level?

10. What controls are currently in place for cyber assets when the MARSEC level is increased? Are the controls all based on physical security?

11. For conducting intelligence and information sharing regarding cyber threats? Does the Port/Facility have a procedure for receiving, analyzing and integrating cyber threat information from open or closed threat intelligence sources to protect from known or eminent cyber attacks?

12. Does the Port/Facility have a procedure for sharing their specific cyber threat / cyber attack information to the DHS National Cybersecurity and Communications Center (NCCIC), State Fusion Center, a representative Information Sharing Analysis Center or Organization (ISAC /ISAO)?

13. Does the Port/Facility have an automated mechanism for submitting and receiving cyber threat intelligence information to Fusion centers, FBI, local law enforcement, etc.?

14. Does the Port/Facility have an automated mechanism for integrating cyber threat data into their organizational protective informational technology (IT)? (i.e. Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) and Cyber Observable eXpression (CybOX))

15. Does the Port/Facility incorporate open/closed threat information into their protective technologies to prevent emerging and/or imminent threats?

16. Does the Port/Facility have a network baseline of what normal traffic for the network is? Does the Port/Facility monitor their network traffic for anomalies or suspicious activity? Identify strengths, gaps, and needs in the intelligence and information-sharing environment of the Port System.

17. What is the Port/Facility's communication plan between its Information and Sharing personnel and its internal or contracted incident response teams during an incident?

18. What is the communication strategy between the Port/Facility and their local law enforcement or Fusion Center, ISAC or ISAO during an active cyber event?

19. What is the communication strategy between the private Port/Facility and their local law enforcement or Fusion Center?

10:00 a.m.

Core Capability Focus Areas: Risk Management and Cybersecurity

Initial Cyber Incident

INJECT 2a - Early in the morning, an email that appears to be from Human Resources about a change to the company's retirement plans was sent to all employee emails. The email instructs employees to click on an attachment to get more information. Approximately 7% of the employees click on the email causing all their machines to get encrypted.

INJECT 2b – Later in the afternoon, the Facility Security Officer (FSO) receives a report that all security cameras throughout the facility have gone down.

INJECT 2c - The access control database used to verify entry into the facility has gone offline. Container trucks / Cargo trucks along with cars containing facility personnel are beginning to create a backlog along the port's/facility's access road.

Facilitator Questions for Inject 2 (Emphasis on Risk Management)

1. Are employees trained on how to respond to a suspected spear phishing attempt?

2. Does your facility have a cyber hygiene training program for your employees?

3. How often does your facility conduct risk assessments and what is the process for conducting the assessment?

4. How do you prioritize your risk? Where does cyber fall on this list?

5. At this time, what resources are made available for employees from a training and response perspective?

6. Has your facility completed a cyber vulnerability assessment? Have business functions been aligned with cyber related controls?

7. Does your facility have safeguards against an insider threat? How about corporate espionage?

8. Do you conduct routine risk assessments? Does your risk assessment process include the identification and prioritization of technology assets to include all business-related data, transactions, and telecommunications (i.e. Information Technology (IT) and Operational Technology (OT) equipment)? In your risk assessment, are your technology assets prioritized by impact if stolen, changed without authorization, or made unavailable?

9. Does your risk assessment consider the loss of physical security technologies such as cameras, access control gates, communication tools or other technology used by physical security personnel?

10. Do your cyber security planners and facility security planners communicate common risks, mitigations, and security measures?

10:20 a.m.

Core Capability Focus Area: Cybersecurity

Facilitator Questions for Inject 2 (Emphasis on Cybersecurity)

1. If your access controls systems appear to be compromised would you notify the Coast Guard? Would you notify adjacent facilities?

2. Who would you contact internally and externally?

3. With a compromised ICS, who / what would be impacted?

4. What potential hazards are created with the systems down.

5. How would it impact other processes and/or operations in the facility?
6. Would IT staff be notified of a suspicious email?
7. Would all phishing attempts hit the end points? Would they have been blocked?
8. Would you be able to determine what domain the phishing attacks originated from?
9. Does your IT department/contractor have the ability to block a specific domain?
10. Has this happened before?
11. Has anyone in your organization had to deal with ransomware?
12. Does IT send out notifications and alerts regarding suspicious emails?
13. Were there any A/V alerts sent?
14. Does the Port / Facility have a risk based cyber security plan? If so, does the plan tie back to the regulations that the Port / Facility follows?
15. What procedures does the Port / Facility have in place to detect unauthorized network activity? How often are these procedures updated?
16. Based on the available information, would the Captain of the Port consider raising the MARSEC Level?

10:45 a.m. Break

11:00 a.m.

Core Capability Focus Area: Situational Awareness

Event Escalation

Inject 3a - IT personnel at a container facility have identified that the Container Shipment Database appears to have been accessed and manipulated. The database has had approximately 300 containers deleted.

Inject 3b – At that same container facility, several cranes that were in the process of off-loading containers from a vessel all of a sudden experiences disruption in their operational capability. Initial exploration looks like all cranes are experiencing a GPS signal disruption which is preventing the cranes from determining its exact location.

Facilitator Questions for Inject 3 (Emphasis on Situational Awareness)

1. How does the IT staff relay intelligence information to external stakeholders? To the Coast Guard?

2. How is the information being distributed to responding agencies?

3. Who would be responsible for painting the big picture? Does the Coast Guard have cyber trained personnel that can connect the dots?

4. What resources are available to help do that?

5. Does the Port / Facility routinely share information to local law enforcement and/or the fusion center?

6. If so, does this information include indicators of compromise (IOC), which are used to identify cyber attacks?

7. Does the Port / Facility know who to share IOCs with at the federal, state and local levels?

8. Does the Port / Facility's information technology and/or cyber security personnel share network situational awareness derived from internal systems with other groups within the port or facility?

9. Would the Port / Facility's management be aware of a small to medium sized cyber attack that was handled internally?

10. Does the Port / Facility employ personnel to monitor social media and the dark web to identify potential threats?

11. Has the Port / Facility ever performed a network vulnerability assessment against web facing systems?

12. If so, was the assessment used to identify the effectiveness of current intrusion detection and/or prevention systems?

11:20 a.m.

Core Capability Focus Area: Risk Management

Post Incident

INJECT 4a - The Port's cyber incident response team has identified several network connected computers that have been infected with a ransomware variant. These infected machines include an engineering workstation used within the Industrial Control System network. The team has physically severed the network connections of all the devices and pulled forensic images of the impacted systems for further analysis and to share with law enforcement.

Inject 4b – The container facility's cyber incident response team has identified several network connected computers that have been compromised by a remote access tool and data stealing trojan. These infected machines contained data sensitive to the container facility. The team confirms that the data was transferred to an anonymized IP address. The team has physically severed the network connections of all the devices and pulled forensic images of the impacted systems for further analysis and to share with law enforcement.

Facilitator Questions for Inject 4 (Emphasis on Risk Management)

1. Having gone through a cyber related event, how does this impact your existing threat assessment?

2. Does this event change the way you prioritize your risk?

3. Based on this scenario, do you believe your threat for a cyber attack is where it needs to be?

11:30 a.m.

Summary

*At this point, the discussion will revisit the key question, "**What are the major consequences of a deliberate and targeted cyber attack event that keeps you up at night**?"*

Do critical areas need further conversation?

This begins a comprehensive examination of the key points discerned during the tabletop discussion, with a view towards identifying next steps.

Summary Discussion and Next Steps

- The summary of today's discussion will be a collective effort.

Questions to consider:

- What were the most significant issues and/or points of discussion from this exercise?
- Was there anything you wanted to say, but didn't have an opportunity or that was not covered in the discussion?
- What should be the top priorities for future efforts in the Port and its facilities? Immediate? Next several months? Years?
- How has your understanding of key homeland security policies and cyber security risk management strategies changed?
- Which areas of the cybersecurity risk management program could be improved in the future?
- Has the placement of catastrophic disaster planning in your list of priorities changed at all based on today's discussion?

Closing Comments

- Exercise Director
- Port / Facility Leadership

12:00 p.m.

Adjournment