Cybersecurity Table-Top Exercise

Inter-American Committee on Ports & United States Coast Guard 2017 Port Security Workshop

April 26, 2017

Agenda

I. Description of the Exercise and Objectives

II. Scenario

III. Provide Injects and Group Reports

IV. Findings Review

Exercise Overview

Objectives:

- Understand interconnected nature of security in seaports; and
- Identify potential areas of concern for both regulatory agencies and port operators.

Methodology:

- Divide into groups based on role as port operator or regulator;
- The scenario will have 3 injects;
- Work in groups to address the questions in each inject; and
- Appoint a spokesperson to provide a brief out.

Scenario

- You are the operator or regulator of Port Hudson. The port is:
  - Operated by a private company with a multi-year contract;
  - A multi-functional port that includes cruise traffic as well as containerized cargo, which is largely transshipped;
  - Confronting a steady amount of narcotics smuggling. Despite the implementation of the ISPS Code and significant investment in physical security measures, the trafficking continues to occur.

Inject 1

- Several cargo shippers are applying pressure to the port and government to further improve security in order to reduce trafficking and thereby make cargo transiting the port less targeted by customs and law enforcement in large trading partners like the US and EU.
- The pressure from shippers includes discussions of re-routing cargo to ports with better security or that comply with ISO 28000 or the WCO SAFE Framework, or that participate in supply chain security programs like C-TPAT and the EU's AEO program.
- Further, cruise operators have expressed concerns regarding the reputation of the port due to the trafficking, but are not threatening to re-route their ships.

Questions

- Identify potential strategies to improve security in the port to reduce trafficking problems. These may be physical, operational, or cyber.
  - What is the role of the port operator?
  - What is the role of the regulators or security agencies?
  - What can be done to make the shippers more confident in the port's security?
  - Is there any single solution?

Inject 2

- After a high profile seizure that included a gunfight with police outside the port when associated raids were being made, the resulting investigation showed that the port's Terminal Operating System (TOS) had been compromised for some time. This compromise involved inside staff accessing the system on behalf of organized criminal groups in order to:
  - Identify containers for the introduction of narcotics based on manifests and routing information; and
  - Dispatch containers to isolated areas of the container yard in order to make them easier to breach.
- As a result, several large shippers have requested a meeting with the port's Chairman and CEO to discuss the immediate cessation of transshipment through Port Hudson and the re-routing of cargo to other ports.
- The cruise operators have also expressed increased dismay as a result of the violence associated with the trafficking and are launching a review of their presence at the port.

Questions

- Identify the potential reasons why the TOS could have been compromised and immediate measures to be taken to enhance the security of the TOS. Key questions:
  - Is this a cyber problem, a physical security problem, or both?
  - What are some of the immediate steps you could take regarding the TOS?
  - How should the shippers' concerns be addressed?
  - What are some of the longer term improvements that need to be made?
  - What are some typical roles and responsibilities for both the operator and the government?

Inject 3

- The investigation into the seizure and shoot-out continues and has now gone international in order to identify the perpetrators of the trafficking. As a result of the investigation, it has come to light that large amounts of cash are being moved back to Port Hudson via the cruise ships. Since the port has already placed a focus on crewmembers as a result of previous drug trafficking cases, the investigation has shown that passenger records have been used to identify potential candidates to carry money ashore in addition to the occasional use of “mules” who make reservations and travel to deliver the cash. The passenger records have been improperly accessed by traffickers with connections back to Port Hudson’s country to identify passengers that meet certain criteria and may be susceptible for recruitment to carry money ashore. This targeting includes:
  - Identifying single, young passengers who have purchased the lowest level of ticket;
  - Identifying passengers who have purchased discounted trips; and
  - Identifying passengers who are first-time cruisers.

Questions

- Identify potential actions to be taken to address the breach of passenger records
- What are the measures that could be taken to improve the cruise ships confidence in the port's ability to deal with the data breach?
- What are the liability issues?

Final Questions

- Where does cyber security begin and end?
- Does the ISPS Code adequately address port security in the digital age?
- Who is responsible for cyber security in your organization? Is that the right place for it?
- What measures can be taken to improve cyber security (and security in general) in your organization?

Facilitators' Comments

- Converged security is the most effective way to address enterprise security in the digital age. This requires:
  - Understanding the problem;
  - Assessing the problem;
  - Organizing to address the problem; and
  - Using converged security to enhance competitiveness.