


AAPA Port Governing Boards

Cyber Management for Ports – Results of Small Port Cyber Security Workshops

MARAD and the CHCP

June 2018

1200 New Jersey Ave., SE | Washington | DC 20590
www.dot.gov

MARAD
U.S. MARITIME ADMINISTRATION

Recent Cyber Attacks

MARAD

- **2017 – NotPetya attack that affected Maersk's global operations** is estimated to have cost over $300 million.
- **2017 - Malaysian bunkering company** defrauded of USD $1 million through the use of spyware.
- **2016 - Pirates hack into a global shipping company's** systems, used the access to locate and retrieve a specific crate on a vessel at sea. Targeted attack, value unknown.
- **2016 - Charter email system** hacked and facilitated fraudulent payment. Vessel was detained on the basis that Charterer's agents did not receive funds for port clearance.
- **2014 - World Fuel Services** suffered a loss of USD $18 million due to fraud.

Recent Cyber Security Issues

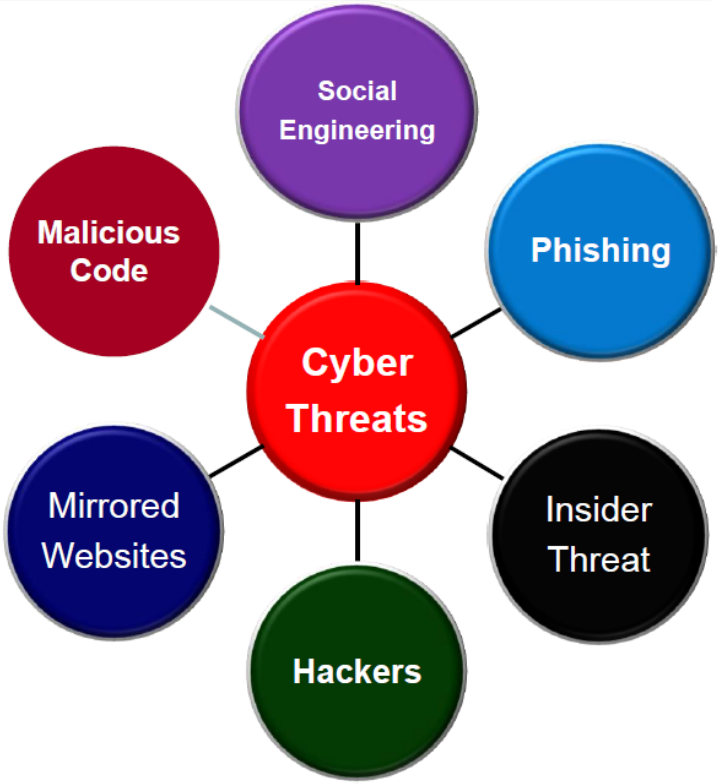
A Recent Cyber Security Editorial in Maritime Executive magazine states that the maritime cyber security landscape is confusing!

- **An I.H.S. Fairplay survey from 2017 found that 47% of those who responded believed that the biggest cyber threats came from inside their organizations.**
- **The survey also revealed that 34% of respondents said their companies had experienced a cyber attack within the previous 12 months (the majority from ransomware and phishing incidents).**
- **Two-thirds of those surveyed stated that their organizations have an IT security policy but that many employees have not had any type of cyber awareness training.**

UNCLASSIFIED

Types of Cyber Threats We are Facing

- Hackers/Intrusion Sets
- Phishing
- Social Engineering or Elicitation
- Malicious Code
- Watering Holes
- DDoS/SQL Injections
- Ransomware



U.S. Maritime Administration (MARAD)

MISSION:
Strengthen the U.S. marine transportation system including infrastructure, industry and labor to meet the economic and security needs of the Nation.

STRATEGIC GOALS:

- **CARGO:** Develop domestic and international transportation opportunities to modernize and sustain a competitive commercial U.S.-flag fleet that ensures the Nation's economic and national security
- **READINESS:** Ensure the availability of a capable U.S. Merchant Marine fleet with modern U.S.-flag vessels, skilled labor and global logistics support to drive the Nation's economy and to meet national maritime transportation requirements in peacetime emergencies and armed conflicts
- **INFRASTRUCTURE:** Support the development of America's ports, shipyards and related intermodal infrastructure as key integrated components of an efficient, resilient and sustainable national transportation system and freight network
- **ADVOCACY:** Advance awareness of the necessity and importance of a strong U.S. Marine Transportation System

Office of Ports & Waterways

MARAD

- Provide Port and Intermodal Planning Assistance
- Access Funding and Financing Options for Port Modernization and Expansion
- Educate re: P3 Opportunities
- Expand domestic movement of freight by waterborne transportation
- Administer Grants and Loans for Projects
  - These services are offered to Port Authorities, State Departments of Transportation, Metropolitan Planning Organizations, and Regional and Local communities.
  - Also offered to privately owned port terminal operators, vessel operators, export industry groups, manufacturers, and other stakeholders.
- **Technology Development – Cargo Handling Cooperative Program**

Cargo Handling Cooperative Program

MARAD

BACKGROUND:

- The Cargo Handling Cooperative Program (CHCP) was established in 1983 by the Maritime Administration (MARAD) to work on the issue of productivity in the marine freight transportation sector. The CHCP was set up as a public-private partnership designed to foster research and technology development to increase productivity of cargo operations. In 1996 the CHCP revised its membership to include all intermodal entities.

ORGANIZATION:

- The CHCP is run by its members with MARAD acting as sponsor and catalyst. The head of the CHCP is a Chair person who is assisted by a Vice-Chair, both are elected by the membership. The CHCP also has a Treasurer to oversee all financial activities of the organization, also elected by the members. The day-to-day activities are performed by a Program Administrator, which is currently done by MARAD.

Cargo Handling Cooperative Program (cont.)

MARAD

FOCUS:

- The overall focus of the CHCP is to assist the intermodal industry with its own technology priorities. This focus is critical for the movement of international and domestic freight. It has been proven that the use of advanced technologies can lead to (1) more efficient infrastructure design, (2) more productive international transportation networks, and (3) better communication and information flows. This approach allows technology to be used in segments of the transportation network to help the total transportation system work more efficiently.

PROJECTS:

- ISO 10374 – Automatic Identification of Freight Containers 1991
- Optical Character Recognition at Marine Terminals 1996
- Chassis Tag Location on Container Chassis 2001
- Electronic Seals for Container Security 2003
- Marine Terminal Productivity Study 2010
- Small Port Cybersecurity Workshops 2018

Cargo Handling Cooperative Program (cont.)

Recently, MARAD and the CHCP have identified a specific group within the maritime sector that has a need for assistance in the increasingly complex area of cybersecurity. Small ports (those with fewer than 50 employees or under 20 million tons of cargo) are having a difficult time navigating the issues that arise from cybersecurity requirements.

Cybersecurity is an evolving area that has many facets. With so much emphasis on data movement and electronic processing, ports, marine terminals and their customers are vulnerable to a number of security problems.

MARAD, through the CHCP, has teamed with Hudson Analytix (HudsonCyber - Cybersecurity + Risk Management Division) to develop a small port cyber security workshop program. MARAD staff contacted several small ports to seek their interest in participating in a workshop to assess their individual readiness under a number of different criteria. The results of the individual assessments are only known by the port. MARAD an the CHCP have been provided a combined view of all three assessments.

Small Ports Cybersecurity Workshop Project

MARAD

- **Geographic Diversity of Ports**
  - East Coast
  - West Coast
  - Great Lakes
- **Variety of Cargo Types**
  - Bulk
  - Project cargo
  - Containers
- **Cargo Tonnage Handled**
  - 1 port < 20 million tons
  - 2 ports < 10 million tons
- **Staff Size**
  - <40 full time staff members

Objectives

1. Identify the current state of cyber risk in and provide recommendations to MARAD- and CHCP-designated ports.

2. Provide MARAD with a summary of project findings and recommendations for how to support small US ports with future cyber risk management activities.

3. Explore how to assist the port industry in the application of cyber security tools for the maritime terminal environment.

Cybersecurity Capability Maturity

MARAD

…what is it?

Project Overview

- **The project evaluated the current state of cybersecurity capability for three small U.S. ports, the results of which, were aggregated to provide common strengths and vulnerabilities, as well as, to mask the identity of the individual ports.**
- **The results of the workshops were compared against established standards to determine cybersecurity capability maturity. The standards used include those from:**
  - U.S. National Institute of Standards and Technology,
  - U.S. Department of Energy/U.S. Department of Homeland Security
  - International Organization for Standardization
  - The Information Systems Audit and Control Association.
- **The assessments did not involve the accessing any computer or information systems within the subject ports.**
- **A number of recommendations have been developed based on these workshops to assist the subject ports and the maritime community at large.**

Common Strengths & Areas for Improvement

MARAD

Change Management	Information Sharing	Physical Security
Cyber Risk Management	Incident Response and Continuity of Operations	Governance
Threat and Vulnerability Management	Commercial	Information and Communications Technology
Situational Awareness	Workforce and Training	Cyber Program Management

Priority Recommendations

- **Establish governance framework**
  - Define both internal and external threats
  - Take a holistic approach to cybersecurity
- **Develop strong cybersecurity program**
  - Need visible backing from Senior Leadership
  - Implement a coordinated cybersecurity program
- **Implement basic course required for all personnel**
  - Training needs to take place at all levels of the organization
  - Training can take many forms: web-based, video, or instructor lead courses
  - Training must be a continuous effort
- **Train executives**
  - A formal program should be established for executives, directors and commissioners
  - Sustain a baseline program to ensure continued emphasis on awareness

Thank You

Robert Bouchard

Director, Office of Port Infrastructure Development

U.S. Department of Transportation

Maritime Administration

Washington DC 20590 USA

202-366-5076

robert.bouchard@dot.gov

Rob Quartel

Chair CHCP

Chairman & CEO

NTELX

1775 Tysons Blvd

Tysons VA 22102 USA

703-356-5050

rquartel@ntelx.com

Andrew Baskin

VP Global Policy & Trade

Hudson Analytix

#2 Aquarium Drive

Suite 300

Camden NJ 08103 USA

856-342-7500

andrew.baskin@hudsonanalytix.com