Inland Marine Expo 2019

Cyber Risk Management

LCDR Dan Mochen
Office of Port & Facility Compliance
Critical Infrastructure Protection Branch (CG-FAC-1)
U.S. Coast Guard Headquarters
“Cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my department and for our country’s security.”

DHS Secretary Nielsen
Cyber Risk Management

- **Coast Guard Cyber Strategy**
  1. Defending Cyberspace
  2. Enabling Operations
  3. Protecting Infrastructure

“*We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation’s critical maritime infrastructure*”
Cyber Risk Management

- **CG-5P Policy Letter 08-16**
  - Reporting Suspicious Activity & Breaches of Security

- Criteria for reporting BoS and/or SA for both physical & cyber related events

- SA: Large, Sustained cyber attacks in an apparent attempt to exploit them

- Reports to the NRC

- National Cybersecurity & Communications Integration Center (NCCIC)
  - Cyber incidents only, do not involve physical or pollution effects
Cyber Risk Management

- “Draft” Cyber NVIC – Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities
  - Guidance on incorporating computer systems & networks into FSAs & FSPs
  - Clarifies 33 CFR 105 & 106
  - 200+ comments on draft NVIC
  - Currently under review
Cyber Risk Management

- **Cybersecurity Framework Profiles**
  - Customize the National Institute of Standards & Technology (NIST) Cybersecurity Framework.
  - Voluntary, non regulatory
Cyber Risk Management

Cyber Awareness Training

- 101 level awareness training
- Familiarity of cyber terms/issues in MTS
- Tailored to AMSC audience
- Available for all audiences

6/8/2018: Marine Transportation System cyber awareness webinar – recording available online

Submitted by Lt. Cmdr. Brandon Link, Office of Port and Facility Compliance

Throughout the month of May, the Coast Guard’s Office of Port and Facility Compliance, in coordination with ABS Group, provided four opportunities for Area Maritime Security Committee members to participate in “Maritime Transportation System Cyber Awareness Training” via webinar. Over 200 AMSC members and port stakeholders participated in the sessions.

In consideration of those who were not able to participate in one of the scheduled webinar sessions, the Coast Guard has made a recording of the training that is available online at the following websites:

- Port and Facility Compliance website
- Portspot – Click on “Maritime Cybersecurity Awareness Webinar” on the left side of the screen, and then the “Maritime Cybersecurity Awareness – May 16, 2018” file on the right
- Domestic Ports Division Cybersecurity website – Scroll down to the “References” section near the end of the page and click on “Maritime Cybersecurity Awareness Webinar” link

This training was developed to provide basic cyber awareness with a focus on maritime facility and vessel operations. The awareness training is intended to provide personnel at all levels of the organization with a basic understanding of cyber terms and systems that may be encountered throughout the Marine Transportation System. The webinar was tailored to the AMSC audience, but is open to anybody with an interest in increasing their cyber awareness.

The Coast Guard is reviewing questions and feedback and will take these into consideration in updates and improvements to this and future cyber-focused training.

For any questions on the material covered in the webinar, or for any technical issues, please contact Mr. Matt Mower, ABS Group, at mmower@abs-group.com, or Lt. Cmdr. Brandon Link, Office of Port & Facility Compliance, U.S. Coast Guard Headquarters.
Cyber Risk Management

• FAA Reauthorization Act
  – “Develop & Implement a Maritime Cybersecurity Risk Assessment Model to evaluate current & future cybersecurity risk that have the potential to affect the MTS or would cause a TSI.”
  – Facility & Vessel Security Plans to include detecting, responding to, and recovering from cybersecurity risks that may cause a TSI

• AMSC Cyber Subcommittee National Meetings
Cyber Risk Management

Commercial Vessels
Office of Design and Engineering (CG-ENG)

End Goal:
Implement a cyber risk management regime based on corporate governance and leveraging existing safety management systems.

Strategy:

- **Vessels**
  - IMO/SOLAS instruments and industry initiatives

- **Facilities**
  - MTSA authority and industry initiatives
Clear path to compliance:
MSC Resolution 428(98)
Maritime Cyber Risk Management in Safety Management Systems

- **Standards Development**
  - Appropriate standards will follow the Guidelines for Cyber Risk Management (MSC/FAL Circ. 3)

- **Incorporation of CRM into SMS**
  - Company selects an appropriate standard and incorporates those practices into their SMS

- **Review of SMS by RO**
  - Recognized Organization (RO) reviews SMS during annual review

- **New DOC issued**
  - New DOC is issued in accordance with MSC Resolution 428(98) prior to 1 January 2021

- **Evaluation during SMS audits**
  - SMS audits will provide feedback and verification
MTS Cyber Threats

- **Industrial Control Systems**
  - Policies & Protocols
  - Built for Safety not Security

- **3rd Party Vendors**

- **Open/Default Passwords**

- **AIS & GPS Spoofing**

- **Spear Phishing**
  - Malware
  - Ransomware

- **Insider Threat**

---

**10/4/2018: National Cybersecurity Awareness Month:**

Cyber threats in the maritime environment

- Phishing/Spear Phishing: Phishing is an attempt to induce individuals to reveal personal information such as passwords and credit card numbers. Spear phishing is a targeted attempt based on who the individual is (i.e., the company they work for). This is accomplished by trying to get an individual to download a file or click on a hyperlink. Users should be wary of emails received from people they don’t know asking them to click on a link or download a file.
# DHS NCATS

<table>
<thead>
<tr>
<th>Service</th>
<th>Duration</th>
<th>Wait Time</th>
<th>Annual Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Hygiene</td>
<td>Ongoing</td>
<td>None</td>
<td>No limit</td>
</tr>
<tr>
<td>Phishing Campaign Assessment</td>
<td>6 Weeks</td>
<td>~ 3 months</td>
<td>32</td>
</tr>
<tr>
<td>Validated Architecture Design Review</td>
<td>1 Week</td>
<td>~ 3 months</td>
<td>50</td>
</tr>
<tr>
<td>Risk &amp; Vulnerability Assessment</td>
<td>2 Weeks</td>
<td>~ 9 months</td>
<td>60</td>
</tr>
<tr>
<td>Remote Penetration Test</td>
<td>4 Weeks</td>
<td>~ 6 months</td>
<td>64</td>
</tr>
<tr>
<td>Red Team Assessment</td>
<td>90 Days</td>
<td>~ 3 months</td>
<td>4</td>
</tr>
</tbody>
</table>

Email: ncats_info@hq.dhs.gov
Resources

- CG Maritime Commons
- CG-FAC-1 Website
- ENG Website
- Homeport