CYBER RISK MANAGEMENT IN THE MARINE TRANSPORTATION SYSTEM

LCDR Brandon Link
10/26/2018: National Cybersecurity Awareness Month – Area Maritime Security Committees

Friday, October 26, 2018

We continue our National Cybersecurity Awareness Month series with a post from the Domestic Ports Division of the Office of Port and Facility Compliance that discusses the important contributions the 43 Area Maritime Security Committees make at local levels to address cyber threats and vulnerabilities. In this post, we focus on the teamwork and cooperation of the AMSCs in Northern New England, the Sault Region, Hawaii and American Samoa, and Charleston, S.C.

10/24/2018: Coast Guard to present during ASTM International's automation and cybersecurity workshop

Wednesday, October 24, 2018

The workshop provides a forum for the exchange of ideas related to the operation of autonomous vessels in the maritime sector, as well as ship automation and cyber risk management in the maritime domain. The objective is to identify potential opportunities for standards and related products applicable to advancements in automation, autonomous shipping, and maritime-specific cyber risk management issues.
Coast Guard Cyber Strategy

Three strategic priorities:
- Defending Cyberspace
- Enabling Operations
- Protecting Infrastructure

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- National Cyber Strategy
- PPD 41: United States Cyber Incident Coordination
- Department of Homeland Security Cybersecurity Strategy
E-Navigation Underway North America 2018

- Maritime Cybersecurity Awareness Webinar
- Information Sharing & Messaging
- Area Maritime Security Committees & Subcommittees
- National Cybersecurity & Communications Integration Center
CG-5P Policy Letter 08-16: Reporting Suspicious Activity and Breaches of Security

- Criteria for reporting breach of security and/or suspicious activity for both physical and network or computer-related events.
- BoS: Includes breach of telecommunications equipment, computer, and networked system security measures.
- SA: Large, sustained attacks on important cyber systems in an apparent attempt to exploit them for nefarious purposes.
- Reports made to the National Response Center.
- National Cybersecurity and Communications Integration Center (NCCIC) – for cyber incidents that do not also involve physical or pollution effects.
Cyber NVIC – Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act-Regulated Facilities

- Providing guidance on incorporating computer systems and networks into FSAs and FSPs.
- Clarifies requirements in 33 CFR 105 & 106.
- Over 200 comments received after publishing draft NVIC.
- NVIC updated based on comments, and is going through review at DHS level.
Cybersecurity Framework Profiles

Customizations of National Institute of Standards and Technology (NIST) Cybersecurity Framework

Voluntary, non-regulatory

Assess where you are at with cyber risk management, where you want to be, how to get there

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Category Unique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td>Protect</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td>PR.AC</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>PR.AT</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>PR.DS</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
<td>PR.IP</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>PR.MA</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>PR.PT</td>
</tr>
<tr>
<td>Detect</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>DE.CM</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>DE.DP</td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Response Planning</td>
<td>RS.RP</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RS.CO</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>RS.AN</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>RS.MI</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RS.IM</td>
</tr>
<tr>
<td></td>
<td>Recovery Planning</td>
<td>RC.RP</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RC.IM</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RC.CO</td>
</tr>
</tbody>
</table>

Subcategory | Informative References
------------|--------------------------------------------------
ID.BE-1: The organization’s role in the supply chain is identified and communicated | COBIT 5 APO01.02, DS206.03, ISA 62443-2-1:2009 4.3.2.3.3, ISO/IEC 27001:2013 A.6.1.1, NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated | COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2, NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | COBIT 5 APO02.06, APO03.01, NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established | COBIT 5 APO02.01, APO02.06, APO03.01, ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6, NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established | ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3, NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
Developing Profiles

Identify industry segment to develop profile

Workshop for stakeholders, subject matter experts, industry trade organizations

Develop the “Mission Objectives”

Map mission objectives to framework’s objectives and sub-objectives

Review each mission objective and subcategory and rate by priority level

Leverage existing standards

Passenger Vessel Operations Profile Mission Objectives

1. Maintain Human Safety
2. Maintain Marine Safety and Resilience
3. Maintain Environmental Safety
4. Maintain Guest Support, Basic Hotel Services
5. Maintain Regulatory Compliance
6. Assure Secure Communications by Function and Mode
7. Optimize and Enhance Guest Experience and Value
8. Maintain Supply Chain and Turnaround
9. Disembarking, Embarking, and Turnaround
10. Coordinate Port Operations
11. Assure (Optimize) Lifecycle Asset Management
12. Maintain Passenger Information and Accounting Systems
13. Manage, Monitor, and Maintain Non-Guest-Facing Back Office Technology
E-Navigation Underway North America 2018

- Assure (Optimize) Lifecycle Asset Management
- Maintain Marine Safety & Resilience
- Coordinate Port Operations
- Disembark, Embark, & Turnaround
- Maintain Operational Efficiency
- Supply Chain and Turnaround
- Maintain Logistics
- Maintain Reliability
- Maintain 3rd Party Integration
- Maintain Personnel/Human Safety
- Obtain Timely Vessel Clearance
- Meet HR Requirements
- Maintain Preparedness
- Maintain Secure Comms
- Maintain Operational Security
- Maintain Consistent & Effective Stakeholder Comms
- Manage, Monitor, & Maintain Non-Guest-Facing Tech
- Maintain Regulatory Compliance (Pass Audits & Inspections)
- Optimize & Enhance Guest Experience & Value
- Maintain Quality of Product
- Maintain Cyber Situational Awareness
- Maintain Passenger Info & Accounting Systems
- Assure Comms by Function and Mode

KEY: ONG Consensus | MBLT | All Offshore | All Consensus | Passenger Vessel
E-Navigation Underway North America 2018

<table>
<thead>
<tr>
<th>Phase I</th>
<th>Awareness &amp; Training</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Awareness in maritime industry</td>
</tr>
<tr>
<td></td>
<td>• Awareness in government (CG, DHS, IMO)</td>
</tr>
<tr>
<td></td>
<td>• Train CG workforce and maritime industry personnel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase II</th>
<th>Corporate Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Industry-led governance regimes to manage cyber risk</td>
</tr>
<tr>
<td></td>
<td>• Third-party consensus standards, best-practices, and training</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase III</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• CG and international standards for CRM</td>
</tr>
<tr>
<td></td>
<td>• Minimum design requirements</td>
</tr>
<tr>
<td></td>
<td>• Align with industry partners, class societies, and internationally</td>
</tr>
</tbody>
</table>
E-Navigation Underway North America 2018

**IMO – MSC/FAL Circ. 3 (May 2016)**

*Guidelines on Maritime Cyber Risk Management* (previously MSC. Circ 1526)

- Establishes high-level guidelines for a holistic, risk management approach to cyber
- Aligns with NIST Cybersecurity Framework

**IMO – Maritime Safety Committee Resolution 428(98) (June 2017)**

- Affirms that approved Safety Management Systems should take cyber risk management into account
- Encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems by 1 January 2021

**Flag State Implementation (June 2017 – January 2021)**

- USCG collaborating with industry to develop a clear path to compliance with MSC Resolution 428(98)
- Development of industry standards, Company implementation, verification, and feedback through the SMS audit process
CG-FAC
- Brandon Link, LCDR: Brandon.M.Link@uscg.mil
- Daniel Mochen, LCDR: Daniel.P.Mochen@uscg.mil
- Charles Blackmore: Charles.T.Blackmore@uscg.mil

CG-ENG
- Kevin Kuhn, LT: Kevin.X.Kuhn@uscg.mil