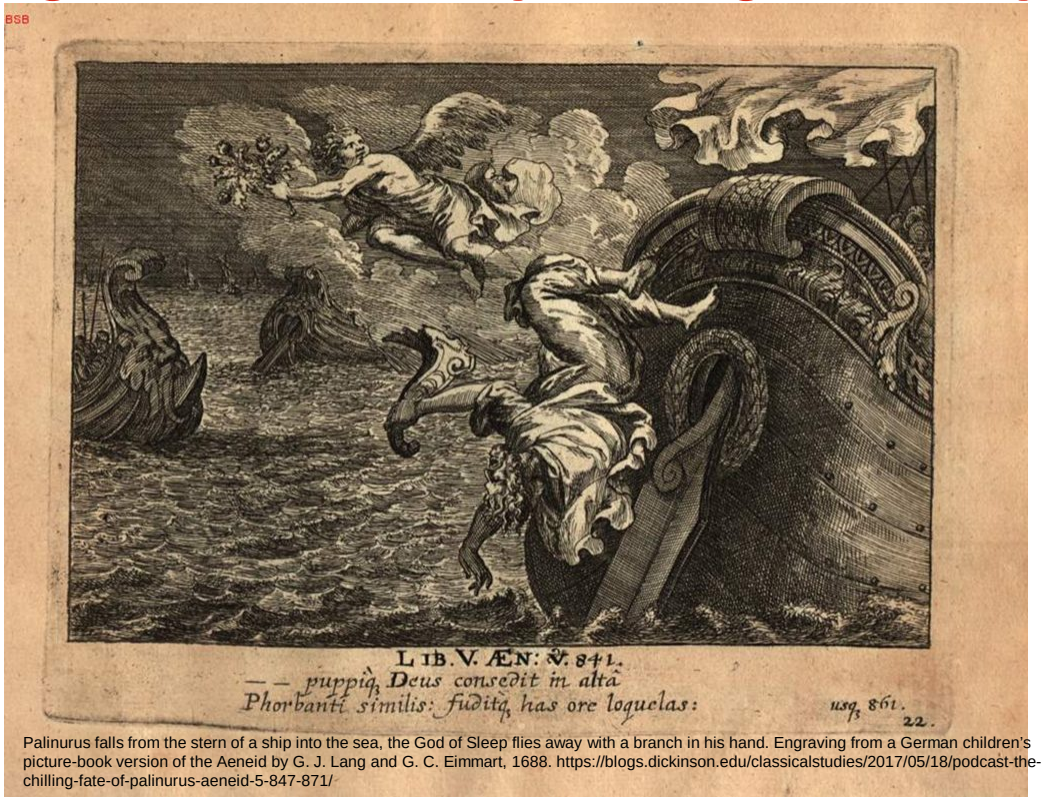
PRESENTATION

IMO Resolution MSC 428(98) - Maritime Cyber Risk Management In Safety Management Systems



Palinurus falls from the stern of a ship into the sea, the God of Sleep flies away with a branch in his hand. Engraving from a German children's picture-book version of the Aeneid by G. J. Lang and G. C. Eimmart, 1688. https://blogs.dickinson.edu/classicalstudies/2017/05/18/podcast-the-chilling-fate-of-palinurus-aeneid-5-847-871/

Implementation in the United States – Coast Guard Work Instruction CVC-WI-027

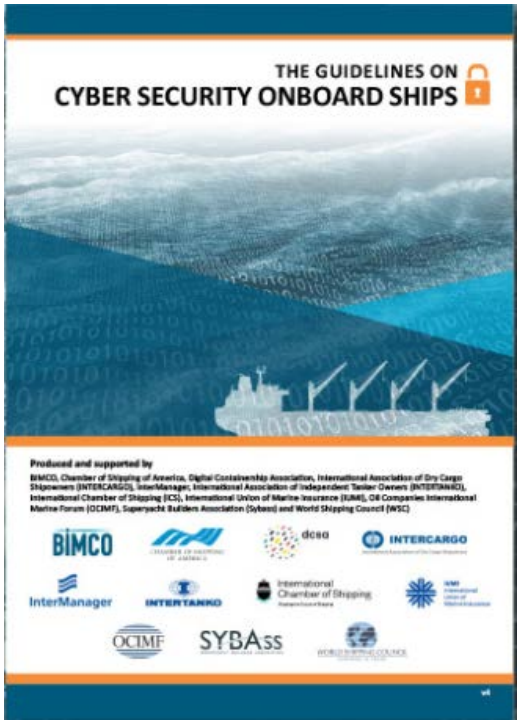
Christopher Hannan
Shareholder
channan@bakerdonelson.com

BAKER DONELSON

EXPAND YOUR EXPECTATIONS℠

IMO Res. MSC 428(98) - USCG CVC-WI-027

- Roughly contemporaneous with the June 2017 IMO Resolution, the IMO also issued MSC-FAL.1/Circ.3 (July 2017) - GUIDELINES ON MARITIME CYBER RISK MANAGEMENT



- January 1, 2021 recommended implementation by flag states – i.e. compliance by first annual verification of ISM Code Document of Compliance after 1/1/21

IMO Res. MSC 428(98) - USCG CVC-WI-027

- Questions as to how flag states would implement the IMO's resolution recommendation – **non-prescriptive, general guidance only**
- 27 October 2020 (Cybersecurity Awareness Month) the U.S. Coast Guard issued Vessel **Cyber Risk Management Work Instruction CVC-WI-027** (updated 18 February 2021), which specifies the U.S. approach to implementing IMO Resolution MSC 428(98)
- Applicable to U.S.-flagged vessels subject to ISM Code (passenger vessels, MODUs, cargo/tanker vessels > 500 GT) and vessels voluntarily opting into ISM Code compliance (Alternative Compliance Program, 46 CFR Part 8)
- Also applicable to foreign-flag vessels calling at U.S. ports/places pursuant to Port State Control inspections
- Safety Management Systems (SMS) must address cybersecurity for "systems affecting safe operation and navigation"

IMO Res. MSC 428(98) - USCG CVC-WI-027

- Two-tier inspection approach: basic cyber hygiene ***observations*** ➔ statutory requirements or technical or operational-related ***deficiencies***

- For technical or operational deficiencies that individually/collectively do not warrant the detention of the ship but indicate a failure, or lack of effectiveness➔ "SMS Related"; internal safety audit and corrective action within three months.

- If objective evidence indicates that the technical or operational-related deficiencies indicate a serious failure, or lack of effectiveness, of the implementation of the SMS ➔ Flag State Detention, SMS external audit required by class prior to ship being released from detention

- Possible shoreside/company audit if (after external audit) nonconformities indicate that the SMS failures exist at the Company level

- WI specifies that USCG inspectors "should NOT direct the ship to create any checklists or procedures with respect to cyber risk management" (i.e. non-prescriptive approach)

- Marine casualty investigation may involve USCG Cyber Protection Team and/or a COTP order restricting/limiting vessel operations.

IMO Res. MSC 428(98) - USCG CVC-WI-027

- Also guidance for Non-SMS U.S. vessels subject to MTSA/MARSEC regulations (Vessel Security Plans (VSPs) and Vessel Security Assessments (VSAs) (MODUs, cargo vessels > 100 GT, passenger vessels, hazardous cargo barges)
- Applicable to MODUs (46 CFR §105(a)), OSVs (46 CFR §105(a)(4)/46 CFR Sub. L) and crew boats (46 CFR §105(a)(5)
  - Also applicable to Sub M towing vessels via TSMS option

"A vessel owner or operator must consider cybersecurity vulnerabilities when conducting the vessel's VSA in accordance with 33 CFR 104.305. **Cybersecurity vulnerabilities should be addressed per 33 CFR 104.305(d)(2)(v) and 33 CFR 104.305(d)(2)(vi). Owners and operators have until December 31, 2021 to address cybersecurity vulnerabilities within their VSA**."

- December 31, 2021 compliance deadline
- Deficiencies ➔ 30 days to rectify, directing the VSO to submit cyber-related issues to the CSO; potential for eventual "no sail" item?

IMO R

2. Questions for MIs to ask during Maritime Transportation Security Act (MTSA) Verifications.

a. *Does your VSP address measures taken to address cybersecurity vulnerabilities?*

- If yes: *Are these measures in place?*

1) If yes: No further action/questions.

2) If no, then ask: *Have you communicated that issue to your CSO?*

i. If yes: No further action/questions required.

ii. If no: Issue deficiency as per paragraph G.3 below.

- If no, then ask: *Has the vessel experienced any cybersecurity events[1] within the past 12 months?*

1) If yes, then ask: *Have you reported these cybersecurity incidents to your CSO?*

i. If yes: Reasonably verify reporting to CSO, then no further action.

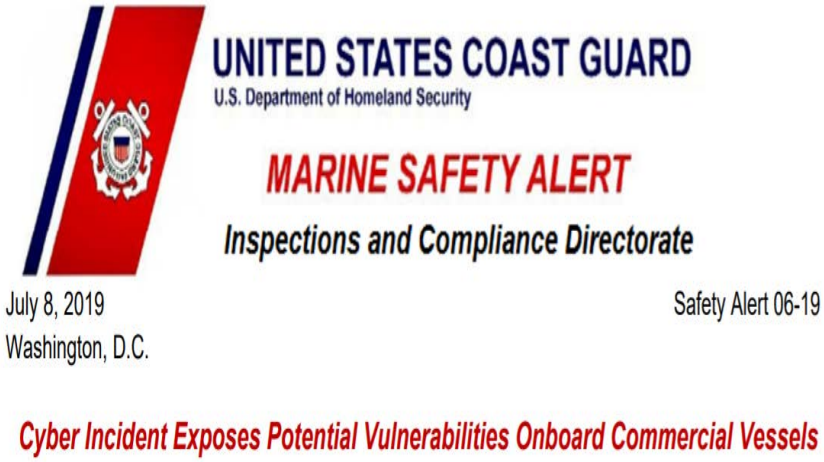
ii. If no: Issue deficiency as per paragraph G.3 below.

2) If no: No further action/question required.

[1] Examples of cybersecurity events include: Intrusions into telecommunications equipment, computer, and networked systems linked to security plan functions (e.g. access control, cargo control, monitoring), unauthorized root or administrator access to security and industrial control systems, successful phishing attempts or malicious insider activity that could allow outside entities access to internal IT systems that are linked to the MTS. Also, instances of viruses, Trojan Horses, worms, zombies or other malicious software that have a widespread impact or adversely affect one or more on-site mission critical servers that are linked to security plan functions.

IMO Res. MSC 428(98) - USCG CVC-WI-027

- ***July 8, 2019*** Marine Safety Alert, USCG stated: "[m]aintaining effective cybersecurity is not just an IT issue, **but is rather a fundamental operational imperative in the 21st century maritime environment**."


UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT

Inspections and Compliance Directorate

July 8, 2019
Washington, D.C.

Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

- "An interagency team of cyber experts, led by the Coast Guard … conducted an analysis of the vessel's network and essential control systems… and found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities."
- *Under Work Instruction CVC-WI-027, this would presumably have resulted in a major deficiency/audit requirement?*

- NIST and USCG (Office of Port and Facility Compliance) have coordinated to develop "maritime specific" Cyber Profiles for terminals/ports– Perhaps one for Vessels in light of IMO implementation?