WINSTON & STRAWN LLP

BLOG

U.S. Coast Guard Reminds Vessel Operators to Report Cyberattack Attempts

JUNE 7, 2019

The U.S. Coast Guard recently released a Marine Safety Information Bulletin alerting the maritime industry to recent cyberattacks against commercial vessels and reminded vessel owners, operators, and masters of the regulatory requirement to report suspicious activity and breaches of security to the Coast Guard National Response Center (NRC) in accordance with maritime security regulations. The reporting requirement applies to all vessels subject to maritime security regulations, including U.S. flag vessels subject to the Safety of Life at Sea Convention and foreign commercial vessels in U.S. waters. However, as noted in U.S. Coast Guard CG-5P Policy Letter 08-16, the cyber-related "suspicious activities" that must be reported are those that indicate targeted cyber incidents involving vessel or waterfront facility systems, as distinguished from untargeted cyber incidents such as "phishing" that are a normal, if annoying and regrettable, part of the normal information technology landscape.

The MSIB was triggered by a recent spate of targeted cyberattack attempts against commercial vessels in the United States in the vicinity of New York. In January 2019, a vessel received an email attempting to mimic a communication from a Port State Control body, with an email address of "port@pscgov.org." The email was sent directly to the vessel's master and requested sensitive information about the vessel, its crew, and its cargo. The master recognized that the email appeared false, and managed the incident under the vessel's security plan for cyber incidents, including a report to the local Coast Guard Sector for investigation. Then in March, a different commercial vessel in the same area received an email on its satellite communication system also simulating a port state control communication, and requested information on whether the vessel had explosive or radioactive cargo aboard. The same vessel received an identical inquiry a month later. In addition, the Coast Guard has received reports of malicious software designed to disrupt shipboard computer systems. In the Mediterranean, NATO has reported that several electronic interferences have been detected, particularly GPS and AIS interference, as well as possible GPS jamming in the Eastern Mediterranean, and has requested vessels to report such instances to the NATO Shipping Centre.

While other flag states have not expressly implemented a reporting regime for cyber-attacks, the International Ship and Port Facility Security Code does require the reporting of "security incidents" that threaten the security of a ship or port facility or any ship-to-ship activity. International Maritime Organization resolutions adopted back in 2017 call for cyber risks to be addressed in vessels' Safety Management Systems by their 2021 annual verifications. Vessel operators should consider including procedures for the recognition and reporting of targeted cyberattack attempts in accordance with U.S. regulations and IMO recommendations.

2 Min Read

Related Locations

Washington, DC

Related Topics

Cyber Security | U.S. Coast Guard | Admiralty & Maritime Law

Related Capabilities

Privacy & Data Security | Maritime & Admiralty

Related Regions

North America