WINSTON & STRAWN LLP

ARTICLE

Window on Washington: Cyber Sets Sail

SECOND QUARTER 2015

This article originally appeared in the Second Quarter 2015 issue of Benedict's Maritime Bulletin. Reprinted with permission.

Automated container tracking and crane systems go haywire in a major U.S. Port, shutting down operations for weeks and wreaking havoc on supply chains across the country. Computer assisted navigation and propulsion systems on a supertanker go dark causing the vessel to break up on the East Coast just before high summer season. An offshore rig's stabilization system fails causing her to tilt at a dangerous angle, shut down production, and potentially discharge large amounts of crude oil. Container tracking and gate appointments are masked and manipulated to smuggle drugs or a dirty bomb through ports undetected. Each of these is an all-too possible scenario resulting from cyber attacks on the maritime sector—and several have happened already.

Cybersecurity is a hot issue in Washington. According to the latest National Intelligence Estimate, the next terrorist attack on U.S. infrastructure is just as likely to be a cyber attack as a conventional terrorist attack, but many sectors of the economy are poorly prepared. Although the Defense Department has been acutely aware of cyber warfare issues for quite some time (how long, only they know) and the Nuclear Regulatory Commission has evolved a regulatory framework following 9/11, there is very little awareness and even less preparedness for cyber attacks upon maritime infrastructure. In the wake of a handful of high priority incidents, such as the Stuxnet worm breach of Iran's nuclear program, and a parade of data breaches against, *inter alia*, Home Depot, Target, and Sony Pictures, other communities are also tuning in, among them the maritime regulators. In February 2013, President Obama issued an Executive Order and companion Presidential Policy Directive calling for improved critical infrastructure cybersecurity across all of Government and emphasizing a cooperative approach with industry. Toward that end, the Executive Order called for the National Institute of Standards and Technology to lead the development of a cybersecurity framework.

1 Min Read

Related Locations

Washington, DC

Related Topics

Admiralty & Maritime Law | Benedicts Maritime Bulletin | Cyber Security | National Security | Window on Washington

Related Capabilities

Maritime & Admiralty

Related Regions

North America

Related Professionals

Bryant Gardner