Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Coast Guard Cybersecurity Guidance Puts Shippers On Notice

By **Erik Dullea, Carlos Rodriguez and Robert Stang** (August 20, 2019, 3:18 PM EDT)

Erik Dullea

Today's commercial cargo ships are marvels of modern technology — a blend of computer navigation displays, electronic sensors, integrated shipboard control systems and telecommunication suites. However, they are just as vulnerable to cyberattack as shore-based computer networks.

The key difference between them is that cargo vessels are in motion. But like attacks on other components of critical infrastructure, attacks on shipboard networks have the potential to cause physical damage within the ship, or to inflict damage to nearby objects outside the ship, if the computers that are compromised are part of the operational control networks rather than the IT networks.

Carlos Rodriguez

Threats to the maritime shipping industry are not new, and they are not trivial. In 2017, A.P. Moller Maersk terminal operations were crippled at various ports worldwide by the "Not-Petya" attack, reducing liftings by 20% for Maersk over the course of two weeks, with approximately $300 million in mitigation and lost business.[1]

In 2018, a ransomware attack degraded the website, email and phone systems for China Ocean Shipping Co.'s American region. The ransomware forced the company to implement a data breach contingency plan that was in effect for more than five days before normal service was restored.[2]

Robert Stang

More recent cyberattacks spurred the U.S. Coast Guard, or USCG, to publish a marine safety information bulletin (on May 24) and a marine safety alert (on July 8) that specifically address cyber adversaries and the vulnerabilities of shipboard computer systems, and the systematic targeting of the maritime shipping industry.[3]

The marine safety alert describes a ship that encountered a significant cyber incident impacting its onboard networks in February 2019. The incident was troubling, in part, because the affected ship is a deep draft vessel that was headed to the Port of New York and New Jersey. Fortunately, the compromised computers were not connected to the ship's operational control systems, but rather handled cargo data and communications with shore-based facilities.

From a maritime safety standpoint, the relatively limited scope of this particular cyber incident could be considered “good news.” However, the USCG notes that in an era when engine commands are sent by mouse clicks and crews rely on electronic charts and navigation systems, it is vital to protect these systems with proper cybersecurity, and in the same manner as crews control physical access to the ship.

Equally concerning, the affected systems show that maritime cybersecurity not only involves pier-side networks — it involves networks operated by harbormasters, ports, freight forwarders, brokers, importers and exporters. A successful cyberattack against an ocean carrier can seriously impact third-party data, which can result in the compromise of underlying buyer/seller proprietary information; financial information, including credit card data; and the compromise of government-protected information such as electronic export information, automated manifest system data, defense trade controls and commerce licensed transactions.

Operation disruptions caused by a cyberattack could also result in an ocean carrier’s inability to book, receive and load cargo, especially if there is interference communicating with the systems that generate authorization to load cargo on vessels in the U.S. Additionally, there could be disruptions in the delivery and release of cargo from terminals, which could result in serious demurrage, detention and storage charges. By way of example, the aforementioned A.P. Moller Maersk attacks caused havoc not only with vessel operations but also with Maersk terminal operations, and with the activities of its related logistics company, Damco.

A common network vulnerability that touches all stakeholders is the industry’s heavy reliance on USB drives. The USCG's recent marine safety alert describes the vulnerability that arises when cargo data is transferred by USB drive on the pier; those drives are routinely plugged into shipboard and pier-side computers without being scanned for malware. Like most federal agencies involved in homeland and national security, the USCG strongly recommends against the indiscriminate use of portable media devices.

The marine safety alert also strongly recommends several other basic security measures that vessel and facility owners and operators must take “to improve the resilience of vessels and facilities, and to protect the safety of the waterways in which they operate.” The USCG’s word choice here is interesting, because it potentially triggers legal obligations for owners and operators.

Black’s Law Dictionary defines seaworthy as the condition of a vessel that is “properly equipped and sufficiently strong and right to resist the perils reasonably incident to the voyage for which the vessel is insured.” In a recent decision, denying an injured crewmember’s claim for punitive damages, the U.S. Supreme Court reaffirmed that seaworthiness is a question of strict liability imposed on the ship owner.[4] For these reasons, the observations below from Dennis Bryant writing for MarineLink[5] are informative:

> Cyber security procedures and protocols must be laid out in the safety management system (SMS) of the vessel and the company. Failure to do so constitutes a deficiency and may result in the vessel being determined unseaworthy. Baltic and International Maritime Council (BIMCO), the largest international shipping association, has developed a new cyber security clause for use in maritime contracts requiring parties to implement cyber security procedures and systems to reduce the risk of an incident.

The February 2019 incident cannot be viewed as an isolated event. Cyber threats evolve rapidly, and the maritime industry must be continually vigilant to this new hazard. In its recent marine safety information bulletin, the USCG described the ongoing threat from cyber adversaries who attempt to gain access to sensitive information such as notice of arrival messages.

As previously noted, the cyber threat does not extinguish pier-side for the vessel or for the parties offloading its cargo. Cyberattacks and data breaches can compromise credit card data and wire transfer instructions, and interrupt future operations. These risks can expose shore-based entities to liability risk under the Shipping Act of 1998's provision covering practices in handling property:

> A common carrier, marine terminal operator, or ocean transportation intermediary may not fail to establish, observe, and enforce just and reasonable regulations and practices relating to or connected with receiving, handling, storing, or delivering property.[6]

Arguably, the safety alert's recommendations for basic security measures "to improve the resilience of vessels and facilities, and to protect the safety of the waterways in which they operate" are setting the bar for what would be considered reasonable cybersecurity standards for the industry. These security measures could in turn trigger culpability pursuant to the legal standards set in the seminal case, T.J. Hooper v. Northern Barge Corp.[7] (known as the "radio-less industry standard case"), as well as by the above-cited Shipping Act of 1998 provision relating to reasonable regulations and practices connected with receiving, handling storing or delivering property.

Technology will remain an important tool for the global maritime community — which means that stakeholders will have to adapt to the modern hazards of the maritime environment. As the USCG notes in its safety alert: "Maintaining effective cybersecurity is not just an IT issue, but is rather a fundamental operational imperative in the 21st century maritime environment."

Erik Dullea is a partner at Husch Blackwell LLP, and a retired captain in the U.S. Navy Reserves.

Carlos Rodriguez is a partner at Husch Blackwell, and transportation counsel to the New York/New Jersey Foreign Freight Forwarders and Brokers Association.

Robert Stang is a partner at Husch Blackwell.

[1] Port of LA Sets Up New Cybersecurity Coordination Center, The Maritime Executive, July 25, 2019, available at https://www.maritime-executive.com/article/port-of-la-stands-up-cybersecurity-coordination-center.

[2] Edwin Lopez, How COSCO responded to a cyberattack on its systems, SupplyChainDive, July 31, 2018, available at https://www.supplychaindive.com/news/COSCO-cyberattack-response-timeline/529008/.

[3] Marine Safety Information Bulletins, USCG, https://www.dco.uscg.mil/Featured-Content/Mariners/Marine-Safety-Information-Bulletins-MSIB/; Marine Safety Alerts,

USCG, https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Investigations-Casualty-Analysis/Safety-Alerts/.

[4] Dutra Group v. Batteron, __ U.S. ___, No. 18-266, at *8 (June 24, 2019).

[5] Dennis Bryant, Maritime Cyber Alert, MarineLink, July 14, 2019, available at https://www.marinelink.com/news/maritime-cyber-alert-468403.

[6] 46 U.S.C. § 41102(c).

[7] T.J. Hooper v. Northern Barge Corp., 60 F.2d 737 (2d Cir. 1932).