Cyber Incidents Targeting Commercial Vessels Highlight Need for Comprehensive Cyber Risk Management

I am getting a little nervous. Ok, VERY nervous.

As reported by Scot Graham (Port Security Specialist and USCG retired Captain at Sector Long Island Sound) to his stakeholders this week, cyber-related risks in the maritime environment continue to be cause of concern. Three spear phishing attempts outlined below indicate a troubling trend toward targeting cargo vessels while underway.

Incident Number 1: On January 26th 2019, a commercial vessel received an email from an individual or entity claiming to represent an official Port State Control body. The email originated from an email address noted as "port@pscgov.org" and was sent directly to the vessel's Captain requesting sensitive information about the vessel, its crew, and its cargo.

The vessel's master was rightfully skeptical about the request and immediately activated elements of the vessel security plan related to this type of suspicious cyber incident. The vessel's Captain reported the incident and forwarded the suspicious email and information to the local USCG Captain of the Port (COTP) for investigation and follow-up.

Incident Number 2: On March 14th, 2019, a different commercial vessel operating in the same area as the previous incident received a SAT-C message by email via the ships Global Marine Distress Satellite System (GMDSS) from an originator claiming to be a U.S. port-specific Port State Control entity. The nature of the inquiry was more direct, requesting information on the nature of the cargo. Specifically, whether the vessel had explosive or radioactive cargo aboard.

Incident Number 3: This same vessel received an identical inquiry again on April 3rd while operating in the same area.

As Captain Graham stated to his partners, cyber technologies enable the Marine Transportation System (MTS) to operate with an impressive record of reliability and at a capacity that drives the U.S. economy and supports national defense, homeland security, and related needs. While cyber systems create benefits, they also introduce risk. Exploitation, misuse, or failure of cyber systems could cause harm to the marine environment or disrupt vital trade activity. As a result, cyber risk management is increasingly important. That begins with a key building block – effective cyber security awareness. - and it culminates in an effective Cyber Risk Management Program. It's not just about "security" anymore, as there will surely be attempts at your doorstep (or dock) as the digital footprint of your organization continues to grow and expand the adversary's attack surface.

I cannot stress enough, the importance of a holistic examination of your cybersecurity from the C-Suite down to the deck plate level, and implementation of a Cyber Risk Management program that uses a proactive (vs. reactive) approach to preventing, preparing and performing when the next attack comes to your organization, be it a port, facility or ship.

If you have not familiarized yourself with the cyber awareness training available, or you want to explore a "no cost" Needs Analysis of your organization, regardless how large or small, or you want to see "no obligation" demo on how a Cyber Risk Management Program can be implemented with an amazing return on investment, let us know at the National Maritime Law Enforcement Academy, by emailing us at Cyber@nmlea.org.