PATRIOT MARITIME COMPLIANCE, LLC

11 July 2019

PMC CLIENT ADVISORY 13-2019

Subject: Cyber Incident Exposes Potential Vulnerabilities Aboard Vessels

To: All Clients

The Coast Guard recently released Marine Safety Alert 06-19 "Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels".

A significant cybersecurity incident recently occurred aboard a commercial vessel. The subsequent investigation, a multi-agency operation lead by the U.S. Coast Guard, noted that while the vessel's network had been significantly impacted, essential vessel control systems had fortunately not been impacted. The interagency team noted that the vessel was operating without effective cybersecurity measures in place, which left critical vessel control systems vulnerable to exploitation.

It was noted that the ship's network was capable of being used by the crew for personal business. Any inadvertent malware loaded onto the ship's official network could cripple the ship's ability to update electronic charts, manage cargo data, and/or prevent the vessel from carrying out ship's business with their company, their agents, and government authorities.

The Coast Guard urges the maritime community to recognize this potentially crippling threat and implement cyber security measures designed to keep the ship's systems safe.

The Coast Guard **strongly recommends** that vessel and facility owners, operators, and other responsible parties take the following basic measures to improve their cybersecurity:

Segment (separate) your networks: A single shipboard network allows those with malicious intent to access the full network, jeopardizing the entire system. The use of sub-networks restricts access within the system, potentially limiting exposure to critical systems.

Use "per-user" profiles and passwords: Eliminate generic log in credentials for the ship (i.e. "Captain", Chief Engineer", "Crew") and create a network profile for each crewmember. Require the use of passwords or "smart IDs" to access the network using "user" level accounts, and limit access/privileges to only what is required to do his/her job. Additionally, PMC recommends that crewmembers be trained to lock their screens when stepping away from the computer, and the enabling of the screen saver or lock screen after a short period of inactivity, combined with the "password required to unlock" feature enabled. The use of "Administrator" accounts should be restricted to those who must have this higher access level.

Treat **ALL** external media (i.e. flash drives) with caution. Flash drives (a.k.a. thumb drives, USB sticks, USB drives, etc.) are routinely used to transfer cargo data, chart and publication updates, the printing of documents for auditors, etc. It's critical that computer systems be set up to automatically scan and cleanse external media before access is allowed. Executable (.exe) files should **NEVER** be run unless it's a known program that's from a trusted source.

Install and keep up to date anti-virus software: This basic step can stop problems before they start. We have seen instances where anti-virus software was installed on a ship's system, but it's rarely (if ever) updated. If this software is not kept up to date, it can be like not having the anti-virus software installed at all.

Keep your systems up to date: Using current operating systems and keeping them patched (updated) is a must. These updates often close critical operating system vulnerabilities, which can be exploited by malicious persons. We have seen instances where the ship's operating system is still Windows XP. While upgrading may be expensive, a crippled computer system can be even more expensive. If an older operating system MUST be used to operate legacy software such as cargo or damage stability programs, it's very important the computer(s) be isolated from the rest of the network. This could be a separate (stand-alone) computer/system, or isolation with strict limited privileges within a subnetwork.

The Coast Guard and PMC strongly recommend that vessel and facility owners and operators have a cybersecurity assessment conducted, and that the results be acted on quickly. We've all seen the results of a major carrier's cyberattack, with the resulting cost and damage to their reputation. Don't let this happen to your company and your vessels.

Please contact our office if you have any questions for PMC.

Yours Truly,

Richard M. Naccara
President