CSCMP hottopics

OCTOBER | 2019

Evolving Threats on the Open Seas: An approach to maritime cyber risk management

By Joshua Berg, Cybeta

CSCMP

Educating and Connecting the World's Supply Chain Professionals.™

Over 90% of the world's goods are shipped via ocean vessels and as the maritime industry becomes increasingly reliant on technology and data, there is a notable increase in cyber risks. Convincing shipowners that information security is worth the investment is challenging because security is an investment for long-term profitability.

Modern vessel navigation and propulsion systems, integrated cargo handling and container tracking systems at ports and on-board ships, and shipyard inventories and automated processes, are all controlled using software that is fundamental to business operations. Highly-skilled threat actors have demonstrated the ability to penetrate the systems used by the maritime industry, with potentially disastrous consequences.

This article provides an overview of information security compliance in the maritime industry, emerging threats from nation-state actors and organized criminals, and maritime cybersecurity risk management.

MARITIME SHIPPING GLOBAL COMPLIANCE

Many shipowners underestimate the extent and complexity of cybersecurity regulations, which can impact bottom lines. In 2011, the European Union Agency for Cybersecurity assessed that the maritime sector's cybersecurity awareness was "low to non-existent" and the focus of nearly all security measures was on physical systems. This assessment was evident as one of the industry's highest-profile cyber-attacks was against container shipping company, Maersk, that occurred in 2017. In the days after Maersk was hit, the company estimated that its losses might run to US$300 million.

In June 2017, the International Maritime Organization (IMO) adopted Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems. The IMO also approved guidelines on cyber risk management, which focus on identifying the systems, data, and capabilities that pose a risk to operations.

The IMO has given shipowners and managers until 2021 to incorporate cyber risk into ships' safety management systems. Owners risk having ships detained if they have not included cybersecurity in the ISM Code safety management on ships by January 1, 2021.

These regulations should ensure that cybersecurity is top of mind, with a firm mandate from senior management. With growing customer demand for faster, more streamlined services that afford integrated and end-to-end logistics, shipping organizations are facing increasing pressure to operate more efficiently due to overcapacity in global markets. There may be a temptation to leave out cybersecurity.

With growing customer demand for faster, more streamlined services that afford integrated and end-to-end logistics, shipping organizations are facing increasing pressure to operate more efficiently due to overcapacity in global markets.

BIGGER AND MORE SIGNIFICANT THREATS ON THE HORIZON

The majority of cyber-attacks have been driven by an attempt to obtain personal or financially sensitive data. As threat actors continue to look for security gaps, the attack surface of ship owners continues to expand. The attack surface can be divided into two significant areas:

- The threat to maritime vessels
- The threat to the ports and automated shipping manifest

Vessels are singled out because these are the top priority for every shipowner as the assets that make money and must be protected. Several common vulnerabilities can be found in onboard systems:

- Obsolete and unsupported operating systems
- Outdated or missing antivirus software and protection from malware
- Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords
- Shipboard computer networks that lack boundary protection measures and segmentation of networks
- Safety-critical equipment or systems that are always connected with the shore side
- Inadequate access controls for third parties, including contractors and service providers

"A ship is safe in the harbor, but that's not what ships are for" — William G.T. Shedd

NATION-STATE ACTORS TARGETING SHIPPING COMPANIES TO CIRCUMVENT SANCTIONS

There is a broad range of reasons to hack a ship; one reason if for extortion. Intelligence collection dating back to at least 2014, provides detailed coverage of the significant nation-state threat actors such as China and the DPRK that continue to exploit the maritime industry. Campaigns by Chinese threat actor TEMP. Periscope (aka Leviathan) used a combination of unique and open source tooling to target the maritime and defense industries for espionage purposes.

A 2019 Insikt Group intelligence report describes a blockchain scam that experts assess with high confidence was conducted on behalf of North Korea against a maritime shipping target. A blockchain application called Marine Chain Platform was supposedly an asset-backed cryptocurrency that enabled the tokenization of maritime vessels for multiple users and owners. Marine Chain is part of a network of enablers throughout the world that assist North Korea in circumventing international sanctions. Users on deep and dark web forums pointed out that www.marine-chain.io was a near mirror image of another site, www.shipowner.io.

What makes Marine Chain stand out from common cryptocurrency or blockchain scammers is that employees of the shipping company have been connected to Singaporean companies that have assisted North Korean sanctions circumvention efforts since at least 2013.

These connections to the Marine Chain Platform mark the first time this vast and illicit network has utilized cryptocurrencies or blockchain technology to raise funds for the North Korean government. Broadly, these types of cryptocurrency scams fit the template of the low-level financial crime described by defectors that has plagued South Korea for years, and that the international community is just beginning to track.

CSCMP™
Educating and Connecting the World's Supply Chain Professionals.™

As technology develops, particularly the interconnectivity of devices and applications, risk by association is amplified, and a thorough understanding of cyber trends is critical.

MARITIME CYBER RISK MANAGEMENT

The goal of maritime cyber risk management is to support safe and secure shipping. Threat intelligence professionals recommend continuous threat analysis that identifies threats that are presented by malicious actions (e.g., hacking or the introduction of malware) or the unintended consequences of benign actions (e.g., software maintenance or user permissions).

The exposure or exploitation of vulnerabilities in information technology systems could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g., improper use of removable media such as a memory stick).

Elements of a Maritime Cyber Risk Assessments physically test and assess the Information Technology (IT) and Operational Technology (OT) systems onboard, including:

- Identification of existing technical and procedural controls to protect the onboard IT and OT systems
- Identification of IT and OT systems that are vulnerable, the specific vulnerabilities identified, including human factors, and the policies and procedures governing the use of these systems (the identification should include searches for known vulnerabilities relevant to the equipment, the current level of patching and firmware updates)
- Identification and evaluation of key shipboard operations that are vulnerable to cyber attacks

DEFENDING SHIP TECHNOLOGY

Cybeta analysts recommend that ship owners and port security apply in-depth vulnerability assessment techniques to critical segments of the software that controls container shipping and the terminal operating system (TOS). For the most part, shipboard networks do not pose a significant risk until they are targeted by attackers who aim to compromise operations.

As technology develops, particularly the interconnectivity of devices and applications, risk by association is amplified, and a thorough understanding of cyber trends is critical. Good threat intelligence practice is as much about awareness of your affiliates' risk exposure as it is about your own exposure.

Cybeta offers unique ways to stay informed in this aspect of the threat landscape. CyberHelm Maritime Risk assessments allow threat intelligence teams to analyze and segregate vulnerable technologies while still being able to see trends from cyber attackers and methods across the entire threat landscape.

Cybeta analysts assess attacks on software that occur worldwide, targeting individuals, corporations, and governments alike. Vulnerabilities in the software that supports critical infrastructure, such as power grids or maritime container shipping, can have even more severe consequences. The key to the prevention of cyberattacks is through a comprehensive Maritime Cyber Risk Management Program. Contact us to learn how this program helps companies like yours find the right data to integrate directly into existing security controls, threat hunting, or incident response systems and processes.

CSCMP™

Educating and Connecting the World's Supply Chain Professionals.™

ABOUT CYBETA™

Founded in 2019, Cybeta offers a suite of Cybersecurity products and services designed to help you keep your business off the Cyber 'X'. Based on decades of detecting and thwarting the activities of even the most advanced attackers, Cybeta delivers the substantive intelligence you need to make preemptive strategic and operational decisions. Think in terms of over-the-horizon visibility coupled with enhanced peripheral vision.

About CSCMP Hot Topics

Issues of *CSCMP Hot Topics* may include early results from ongoing research being conducted for CSCMP or other organizations; new supply chain practices, thought-provoking ideas, or emerging trends; discussions of changes in the broader business and regulatory environment that may impact the supply chain and logistics field.

CSCMP™

Educating and Connecting the World's Supply Chain Professionals.™