RMSC
YOUR GATEWAY TO MARITIME BUSINESS

EXPERT OVERVIEW

NOVEMBER 2023

CYBERSECURITY IN THE MARITIME INDUSTRY: NAVIGATING TROUBLED WATERS

As we all know, the maritime industry is increasingly becoming a target for cybercriminals, especially as it remains the backbone of global trade. Regulatory frameworks from the International Maritime Organization (IMO) European Union exist, though the adoption rate of cybersecurity measures must be faster.

The growing sophistication of cyber threats, many using Artificial Intelligence (AI), only adds to the urgency. The danger for large ports like Rotterdam, Singapore, and Los Angeles is becoming even more of a concern, which faces unique challenges, including handling of illicit goods and severe disruption to supply chains.

The maritime industry's cybersecurity challenges are uniquely complex, given the sector's operational intricacies, global reach, and strategic importance. The maritime sector is also on the cusp of a digital revolution, fueled by the promise of autonomous shipping.

Autonomous vehicles pose new cybersecurity risks - from software vulnerabilities, hacking of electric charging stations till unprecedented challenges.

These self-operating vessels will rely heavily on AI, sensors, and real-time data analytics, dramatically increasing potential cyberattacks. They will also operate in international waters and must contend with varied - and sometimes conflicting - regulatory landscapes and jurisdictions.

IMO GUIDELINES AND EU DIRECTIVES

The IMO guidelines, operational from January 2021, focus on making cybersecurity an integrated part of the Safety Management System (SMS) for vessels. The EU's NIS Directive (EU26) and Cybersecurity Act (EU27) also provide a legal framework that imposes new cybersecurity standards on essential services, including maritime – this comes into force in 2024.

Despite these measures, the industry needs to adapt faster. The existing infrastructure, being legacy systems, often needs to support seamless integration of cybersecurity solutions; financial constraints and lack of expertise further slow the uptake. Also, attitudes within the industry need to catch up on the uptake of even the basic cyber security measures, and corners are cut when it comes to implementing regulatory frameworks.

Cyber threats have evolved from simple malware to sophisticated Advanced Persistent Threats (APTs), ransomware, and spear-phishing attacks. AI is increasingly used to adapt and evolve tactics, making traditional cybersecurity measures inadequate.

CHALLENGES & SOLUTIONS FOR MAJOR PORTS

Ports like Rotterdam, Singapore, and Los Angeles are hotspots for regular trade and targets for illicit activities. Smuggling of contraband, narcotics, and even human trafficking often occur through cargo containers. Cybersecurity lapses can compromise cargo tracking systems, making it easier for illicit goods to slip through the net.

With ports and related facilities becoming ever more connected and digitally aware, the risks are becoming greater for unauthorised data access or suffer complete cyber-attack, and even companies potentially losing the ability to control critical systems and infrastructures. Ports and maritime facilities have become the virtual battleground where major disruption can cause shock waves through the entire global supply chain of a city and/ or country.

Regular vulnerability assessments can identify gaps in security systems before a breach happens. These assessments should be combined with a comprehensive risk assessment that prioritises vulnerabilities. Based on the potential damage they can cause, the risk assessment will

This RMSC Expert Overview is written by Remie Kalloe & Campbell Murray (remie.kalloe@cyber.dockside.ai).

help allocate resources effectively and mitigate risks. Utilising web threat intelligence services can empower maritime companies to predict and prevent future attacks, allowing them to move from a reactive to a proactive stance and better understand the threats external to the business. Maritime companies must not hesitate to engage cybersecurity firms with specialised maritime knowledge.

A game changer will be to have certified consultants as an industry standard. "Cyber.Dockside.ai, with its certified maritime cyber auditors, assists companies in implementing targeted solutions, offer actionable (realtime) insights, and provide continuous support to improve the cybersecurity landscape effectively. They also assist ports, shipping companies and third parties to get their consultants certified".

Cybercriminals are not only becoming more aggressive, but also increasingly sophisticated. Gone are the days when a simple firewall could protect a network.

ROLE OF AI: A DOUBLE-EDGED SWORD

AI isn't just a tool for cybercriminals; it is also being harnessed for cyber defense. AI algorithms can analyse large volumes of data to detect anomalies, enabling faster response to cyber threats. AI can also predict potential future threats based on past patterns, allowing for proactive defense measures. However, the same technology also poses a risk when in the hands of malicious actors. AI can be used to automate attacks, making them more efficient and more challenging to detect. For example, AI-driven social engineering attacks can trick employees into revealing sensitive information, leading to security breaches.

The maritime industry stands at a critical juncture. While guidelines and regulations are being rolled out, the effectiveness lies in quick and thorough implementation. A multi- faceted approach, encompassing regular vulnerability and risk assessments, specialised expertise, and advanced threat intelligence, is essential to navigate the complex cybersecurity landscape

The unique challenges the large ports face add another layer of complexity to the cybersecurity equation. These ports must not only safeguard against cyber threats but also be vigilant about the risks posed by illicit goods that pass through their gateways. Thus, maritime cybersecurity isn't merely an IT issue but a holistic challenge that impacts operational integrity, safety, and national security.
With international trade and global security at stake, adopting a robust cybersecurity framework is not just advisable but imperative. By embracing a layered, comprehensive approach, the maritime industry can comply with existing regulations and fortify itself against the constantly evolving threats it faces.

REGULATORY FRAMEWORK

IMO Guidelines on maritime cyber risk management
The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management.

EU NIS Directive
The NIS Directive is EU-wide cybersecurity legislation harmonizing national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU.

EU Cybersecurity Act
The Cybersecurity Act gives the European Union Agency for Cybersecurity (ENISA), a permanent mandate and strengthens its role. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of digital products and services in Europe.

RMSC
YOUR GATEWAY TO
MARITIME BUSINESS

CONTACT

ROTTERDAM MARITIME SERVICES COMMUNITY

rotterdammaritimeservices.com
info@rotterdammaritimeservices.com