The Information Authority for the Workboat • Offshore • Inland • Coastal Marine Markets

Volume 32 • Number 11

Marine News

NOVEMBER 2021

www.marinelink.com

GREAT WORKBOATS of 2021

Electrification
Leading the charge

Inland Waterways
A crucible of issues

Offshore
Maritime for the win(d)

Column

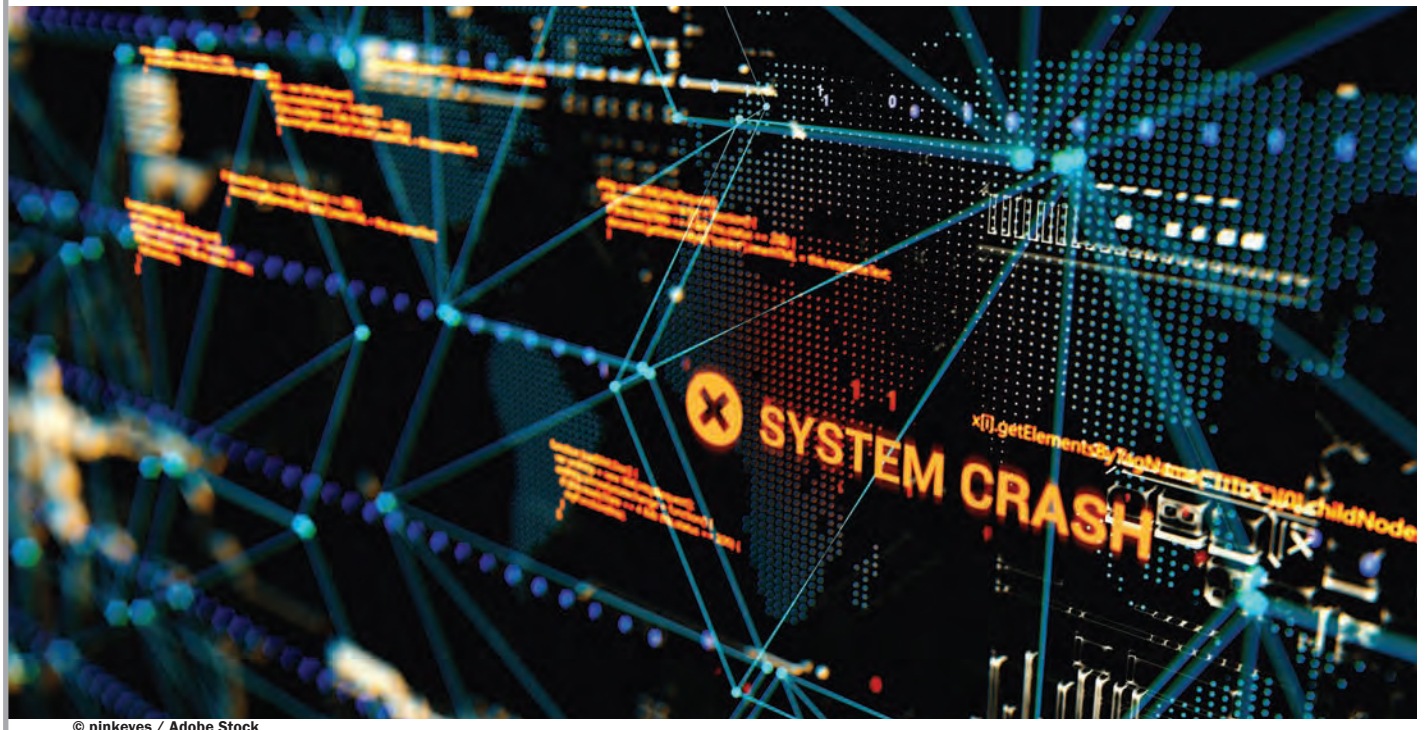
Cyber Security

Maritime Cybersecurity:
Prepare, Detect and Respond

By Vanessa C. DiDomenico, Maritime Associate, Blank Rome

At a time when the world has become more aware than ever before about the vital importance of the world's ocean shipping fleet, which carried supplies, merchandise and much needed personal protective equipment during the COVID-19 pandemic, an increased risk from a different threat, cyberattacks, presents a set of new challenges.

According to Israeli cybersecurity specialist Naval Dome, since February 2020, there has been a 400% increase in attempted hacks on the maritime realm, coinciding with a period when the maritime industry turned to greater use of technology and working from home due to the Coronavirus pandemic. Increased phishing attempts, malware and ransomware attacks can be attributed to the changes in operations and procedures during the travel restrictions and operational hurdles encountered during the pandemic. These global challenges resulted in a move by the U.S. to bolster the federal government's cybersecurity practices and contractually obligate private sector to align with such enhanced security practices. For instance, the ransomware attack on Colonial Pipeline, which controls nearly half the gasoline, jet fuel and diesel flowing along the East Coast, prompted President Biden to sign Executive Order (EO) on "Improving the Nation's Cybersecurity (14028)" on May 12, 2021. A comprehensive overview of President Biden's EO can be found here. On August 25, 2021, the President also held a cybersecurity summit with leading tech company and Wall Street banking executives to discuss cybersecurity concerns.



The Colonial Pipeline ransomware attack provides important lessons for critical infrastructure providers in the maritime industry on being prepared for cyber-attacks. It still remains a mystery how the attacker, DarkSide, first broke into Colonial Pipeline's business network, but recent reports speculate that the pipeline was taken offline because there was no separation between data management and the pipeline's actual operational technology. "Other pipeline operators in the United States deploy advanced firewalls between their data and their operations that only allow data to flow one direction, out of the pipeline, and would prevent a ransomware attack from spreading in." In this case, the attacker did not aim to take hold of the pipeline, but held the data for ransom. The ransomware attack on Colonial Pipeline illustrates the need for separate, offline backup systems and cyber incident response plans.

Similar to the Colonial Pipeline attack and other recent cyber incidents, a targeted cyber-attack upon a sizeable ocean carrier or its supply-chain network could cripple significant segments of the world's transportation capacity to deliver essential goods. We have seen during the COVID-19 pandemic the effects of hindered supply chains, scarce products on store shelves, and long lead times for integral components. To help address the need for increased action against cyber-attacks, the International Maritime Organization (IMO) Maritime Safety Committee, at its 98th session in June 2017, adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The Resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after January 1, 2021. Additionally, the IMO has issued MSC-FAL.1/Circ.3, 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. The Baltic and International Maritime Council (BIMCO) has also published its own Guidelines on Cyber Security Onboard Ships to aid shipowners and ship managers meet the IMO requirement to implement cyber-risk management in their safety management systems. The maritime community should review

these guidelines and implement strategic objectives.

Given the digital revolution that has been taking place in the maritime industry, ships are more connected now than ever before. While the increased connectivity and system integration aids in operational, commercial, and safety efficiencies, it also enlarges the attack surface available to bad actors seeking to exploit vulnerabilities for potential cyber-attacks. There are increased risks for maritime cyber-attacks because shipboard systems and networks are often interconnected with other onboard or remote systems and the internet, which constantly interface with international contacts of all kinds. Both new and old vessels can be susceptible to cyber incidents. Newer vessels are being branded as "smart" ships with thousands of sensors, remote monitoring and troubleshooting, and artificial intelligence capabilities to analyze data in real time. These vessels integrate information technology systems with operational technology systems, thus increasing the exposure of these interdependent systems to cyber incidents. Older ships that are not as sophisticated could still experience a cyber incident because of obsolete operating systems that can no longer be updated, missing or outdated anti-malware software, insufficient security protocols and safeguards (including employee mismanagement of the network and the use of default administrative accounts and simple passwords), integrated computer systems that lack safeguards and network segmentation, systems that must be connected to a server on land to function correctly, or are always connected to a system on shore that is not secure, and unsecure access controls for service providers and contractors. Thus, it is vital to invest in cyber assessments to identify potential areas of weakness to combat potential threats.

The large maritime-cyber ecosystem, consisting of shipboard automation and communication systems, cargo and passenger manifests, port operations and other supply chain members, needs to remain vigilant and proactive by performing cybersecurity training and simulated tests, deploying defenses and developing incident response plans. Defenses require continuous improvement and there is no one-size-fits-all approach. Both procedural and technical countermeasures are needed, and a layered approach is essential. Possible defenses include: backup and data recovery capabilities, multi-factor authentication and access controls, anti-malware tools, robust network monitoring processes, use of Virtual Private Networks (VPN), maintaining software upgrades, patches and maintenance schedules, email and spam filtering, providing security awareness training to personnel and maintaining and testing an incident response policy and physical security to restrict access to shipboard areas. Shipowners, charterers and seafarers also have vital roles to play. Shipowners need to ensure there are prevention, detection and response plans in place. Shipowners and charterers need to understand who bears the risk if a cyber incident occurs that results in delays, damage to the vessel or ransom payments. Shipowners should understand the extent of insurance coverage for cyber incidents and potential losses due to third-party liability. Seafarers should follow company compliance plans and policies to protect onboard systems from phishing attempts and eliminate other opportunities for potential cyber breaches through shore visits, and ship-to-shore interfaces and remote access. Ship managers should also ensure the proper contractual language is inserted for third party suppliers and agents to protect and secure sensitive data and information, and that contractors are properly vetted.

As shipping continues to move towards remotely operated and autonomous driven vessels, stakeholders and governments must collaborate to identify new risks and regulatory gaps. The need for new tools and collaboration to protect against cybersecurity incidents is paramount, as the ecosystem is only as strong as the weakest link. For example, Blockchain and other encrypted solutions could aid in the safety and security of maritime transactions. Not only does Blockchain simplify and provide transparency into fragmented shipping and logistics processes, Blockchain does not have a centralized server, thus reducing the chances of malicious cyber-attacks. Blockchain also reduces inefficiencies, such as error-prone manual exchanges between numerous parties. Furthermore, investment is needed. Developing nations will require support to ensure resilience throughout the supply chain against potential future disruptions. Maritime cybersecurity is a topic that will continuously change course depending on how the industry, and key stakeholders prepare, detect and respond.