NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWSLETTER
January 2021 (Edition 2021-1)

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This newsletter will be e-mailed to members of the Northern California Area Maritime Security Committee and posted on the Coast Guard's HOMEPORT portal within the Sector San Francisco port area.

IF YOU SEE SOMETHING, SAY SOMETHING

To report a crime in progress, call 911 or your local police department. To report maritime related suspicious activities or breaches of security call the National Response Center (NRC) at 800-424-8802 or if a **cyber-attack** to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870. After calling the NRC or NCCIC call the Captain of the Port, San Francisco, at 415-399-3530.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **Maritime Industry Remains Vulnerable to Cyber Attacks** – discusses how a vulnerable system which is "infected" can allow access to multiple shipboard systems and the need for a common "industry code" concerning cybersecurity.
- **All four of the world's largest shipping companies have now been hit by cyber-attacks** – discusses the impact of ransomware on the shipping industry.
- **Maritime cyber-attacks are increasing** – discusses the convergence of information technologies (IT) and operation technologies (OT) and their, now common, vulnerabilities

- **Maritime Industry Rocked by Cyber-Attacks** – discussion about various cyber-attacks and trade disruptions.
- **California Cybersecurity Integration Center** – is the State of California's center for cybersecurity and assistance with cybersecurity related issues.

MAIN ARTICLES

Maritime Industry Remains Vulnerable to Cyber Attacks, By John Grady, USNI News, 28SEP2020

While handling 90 percent of the global economy daily, maritime industry ashore and afloat remains increasingly vulnerable to cyber disruptions and attacks from "ne'er-do-wells and bad actors" that threaten financial markets and the country's national security, the head of the Maritime Administration said last week.

Lacking a coordinated code affecting all modes of transportation and ports and terminals, the "movement of our armed forces" can be disrupted "by a few keystrokes of bad actors" that can affect ship operations, cargo handling and on-shore facilities, retired Rear Adm. Mark Buzby said during a Sept. 24 virtual event hosted by The Atlantic Council.

Cyber disruptions in San Diego and Barcelona port operations in 2018 and continuing ransomware attacks on European transport companies underscore the vulnerability of these interlocked modes of economic movement, Coast Guard Capt. Jason Tama, commander of Sector New York, and Heli Tiirmaa-Klaar, Estonia's ambassador-at-large for cyber diplomacy, added.

Speaking as part of the online forum, Kathy Metcalf, president and chief executive officer of the Chamber of Shipping of America, said all too often cyber security is thought of as the takeover of a ship and ramming it into the Verrazano-Narrows Bridge, which connects Brooklyn and Staten Island at the entrance to New York's harbor.

The real need is for "collaboration" on all the details affecting small links in a supply chain or parts used in maintenance. "The system will only be as good as its weakest link," Metcalf said. The maritime industry includes many links — some more than 30 years old that remain extremely vulnerable, while others are brand new and hardened, Xavier Bellekens, lecturer at the Institute for Signals, Sensors and Communications, University of Strathclyde, said at the forum. Looking only at ships, using open-source information, Bellekens said anyone "can relatively easily … learn very fast about," a ship at sea. Using slides, Bellekens selected one ship operating from a Southeast Asian port and in less than a day followed its course outbound, obtained biographical data on its captain, information on the makeup of the crew, current cargo, destinations and the ship's current position.

The data are potentially useful to hackers, pirates, criminals, terrorists or hostile nation-states.

As he was speaking, Bellekens presented a news photo of the aftermath of a collision at sea between a Russian frigate and merchant ship in Danish waters that occurred the day prior. He used the photo, which was available within a few hours of the mishap, to emphasize the point that "there are many ways to gather open-source information."

Master Mariner Capt. Alex Soukhanov, managing director at Moran Cyber, said that while designers and builders have understood for decades the need for safety, segmentation or compartmentalization in ship work, "cyber and networks" were "not priorities" for years. Those legacy systems are still operating today.

"It really doesn't matter who the bad guy is" in hacking the vessel itself, from propulsion to navigation systems, port management, terminal capacity of cargo, to a maintenance facility's work schedule because "all of these systems are connected together."
Tama said, "we're years behind other sectors," like finance, in understanding these connections and the need for collaboration between ship owners, vessel operators, ship builders and designers, terminal and port authorities, and companies and law enforcement.
The reluctance to collaborate in the private sector and even in public-private partnerships with law enforcement agencies, including coast guards, has been shifting, Metcalf, Tama and Tiirmaa-Klaar agreed.

The impact of ransomware demands in all manners of business — from health care to utilities to transportation — has been a key factor in this shift. Even reducing this to cybersecurity on ships alone, Metcalf said, "not all the ships are the same" because they were built at different times for different operations. An example of "flesh on the bones" for vessels could be drawn from the International Safety Management agreement to improve cybersecurity afloat.

Moreover, Metcalf said the reality aboard a ship is that the first questions a captain or master ask if the ship's operations are disrupted aren't about cyber. They will instead ask about restoring that capability or how to work around it. In addition, most officers and crew "don't realize how important [a part, a system, etc., are] until it's no longer working." For all the activities involved in maritime operations, "you can set up some general principles" and "the right place is in the [International Maritime Organization]," she added.

All four of the world's largest shipping companies have now been hit by cyber-attacks, By Catalin Cimpanu, Zero Day, 28SEP2020

Maritime industry needs to focus more on securing shore-based systems and stop prioritizing the less likely ship-based attacks.

With today's news that French shipping giant CMA CGM has been hit by a ransomware attack, this now means that all of the four biggest maritime shipping companies in the world have been hit by cyber-attacks in the past four years, since 2017. Previous incidents included:

1. APM-Maersk - taken down for weeks by the **NotPetya** ransomware/wiper in 2017.
2. Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.

3. COSCO - brought down for weeks by ransomware in July 2018.

On top of these, we also have CMA CGM, which today took down its worldwide shipping container booking system after its Chinese branches in Shanghai, Shenzhen, and Guangzhou were hit by the **Ragnar Locker** ransomware. This marks for a unique case study, as there is no other industry sector where the Big Four have suffered major cyber-attacks one after the other like this. But while all these incidents are different, they show a preferential targeting of the maritime shipping industry.

"I'm not so sure it's that they're any more or less vulnerable than other industries," said Ken Munro, a security researcher at Pen Test Partners, a UK cyber-security company that conducts penetration testing for the maritime sector. "It's that they are brutally exposed to the impact of ransomware. " After Maersk was hit by the NotPetya crytper, I believe criminals realized the opportunity to bring a critical industry down, so payment of a ransom was perhaps more likely than other industries," Munro said.

Maritime cyber-attacks are increasing, By Anastasios Arampatzis, Tripwire, 22 SEP 2020

The last victim in a long list of cyber-attacks was cruise operator Carnival Corp, who announced on 15 August 2020 that they had suffered from an attack involving files being stolen. According to David Bernstein, chief financial officer for Carnival, the company "detected a ransomware attack that accessed and encrypted a portion of one brands' information technology systems. The unauthorized access also included the download of certain of our data files."

It seems that the ransomware attack included unauthorized access to personal data of guests and employees. The incident may become a costly one for the cruise operator, as it may result in potential claims from guests, employees and regulatory agencies.

This was the most recent event in a series of incidents that affected both shipping companies and ports. Since **NotPetya** caused US$300 million in losses for Maersk, the attacks are increasing at an alarming rate. In 2018, the ports of Barcelona and San Diego fell under attack. Australian shipbuilder Austal was also hit, and the attack on COSCO took down half of the shipowner's US network.

Fast forward to 2020, when the shipping company MSC was hit by malware, which resulted in shutting down the shipowner's Geneva headquarters for five days. According to a US Coast Guard security bulletin, a cargo facility's operating system was infected with the **Ryuk** ransomware. Finally, the OT systems at Iran's Shahid Rajee port were hacked, restricting all infrastructure movements and creating a massive backlog.

- **The convergence of IT and OT systems creates new challenges**

Until relatively recently, topics relating to cybersecurity have been the domain of the IT department. However, securing Operational Technology (OT) is becoming critical for maritime and shipping business, since they rely more on smart, cutting-edge technology. (This is especially true for the digitalized maritime sector, as we discussed in a recent post.)

“All new builds are based on software that runs systems within the ship pertaining to safety and security, and also for monitoring of operations,” says former naval officer Chronis Kapalidis, a maritime cybersecurity researcher at HudsonAnalytix and an analyst at Chatham House. “It’s important that cybersecurity across IT and OT becomes part of a new cyber culture. It shouldn’t be something that ship owners are requesting and pushing the vendors for – it should be something vendors have in place to demonstrate their competitive advantage.”

The IMO recognized the need to make sure that these OT systems are secure. In response, it required that all maritime administrators appropriately address the cyber risk of their Safety Management Systems by January 2021.

Addressing these risks begins with knowing your vulnerabilities and being prepared for a constant increase of cyber threats. Paul Ferrillo, partner at Law firm McDermott, Will & Emery said in a recent webinar that all ports and terminals are attractive targets for cyber attackers. “If you have data, you are a target,” he warned. “You will be attacked and breached – you may already be breached, but you may not know it.”

However, cyber threats that threaten to break the maritime operational reliability and delay cargo delivery carry additional risks. “Infected systems can compromise navigation or propulsion, threatening ship safety itself as well as the marine environment,” reads a recent article by ABB. With cyber-attacks against port operators and shipping companies increasing, “people need to be aware of the threats,” says Scott Dickerson, executive director at Maritime Transportation System ISAC. “It is not just a technology challenge. Some ports do not have a dedicated IT person, so at operational level people need to understand how they are being targeted and make sure they have good cyber hygiene.”

- **Traditional cybersecurity does not work**

The quantity of information transmitted from ship to shore has increased dramatically thanks to advances in maritime communications and an ever-increasing reliance on technology-enabled on-board systems.

“What is interesting is that many operators believe they have this protected with traditional cybersecurity, but the firewalls and software protecting the IT side, do not protect individual systems on the OT network,” says Jonas Blomqvist, General Manager, Cyber Security, Marine Business at Wärtsilä.

Installing an antivirus platform on a vessel bridge navigation system (ECDIS) could very quickly impair and inhibit system performance, for example.

“Operational networks, in contrast to information networks, are measured by their performance level. Their operation cannot be disconnected and stopped. An emergency state in these systems can usually only be identified following a strike and they will be irreparable and irreversible,” adds Blomqvist.

Taking precautions by installing security systems, such as firewalls and detection systems for denial of services attacks and other malware, is crucial but insufficient. Adopting proactive cybersecurity risk management provides an opportunity for shipping companies to differentiate themselves.

- **Maritime cyber resilience is a strategic advantage**

Cyber resilience has emerged over the past years because traditional cybersecurity countermeasures are not sufficient to protect organizations against sophisticated attacks. Preserving both cybersecurity and cyber safety are important because of the potential effect a cyber-attack might have on personnel, the ship, the environment, the company and the cargo. Cyber resilience programs should be able to identify, assess and manage the cyber risks. They must continuously monitor all mission critical systems to detect anomalies, change and potential cybersecurity incidents before they cause significant damage and disrupt the reliability and safety of operational processes. An incident response management program ensures business continuity and helps the maritime and shipping company to continue to operate despite a cyber-attack.

With cyber-attacks increasing in frequency and severity, supposing that maritime and shipping organizations can defend against every potential attack scenario is just wishful thinking. Organizations need to combine cybersecurity with business resilience to be cyber resilient. As the maritime sector continues its digitalization journey, a safer shipping offering is a competitive strategic advantage.

Maritime Industry Rocked by Cyber-Attacks, By Jennifer Diaz and Sharath Patil, 20OCT2020.

The maritime industry has been rocked by a string of cyber-attacks in recent weeks. Two of the most severe incidents involved the United Nation's shipping agency, the International Maritime Organization ("IMO"), and the French shipping company CMA GCM S.A. ("CMA GCM").

These attacks remind the shipping industry about the dangers of such attacks and the importance of cybersecurity compliance. From a trade and customs perspective, such incidents trigger post incident analysis and other measures as part of the U.S. Customs & Border Protection's ("CBP") Customs Trade Partnership Against Terrorism Minimum Security Criteria. We will discuss two of the most severe cyber-attack incidents in recent weeks below and then discuss the trade and customs implications of such attacks.

- **The International Maritime Organization Target of 'Sophisticated' Attacks**

Beginning on September 30, 2020, the UN shipping agency, the IMO, was the target of a cyber-attack which forced the agency to shut down its website and public web-based services. In an October 1 statement, the IMO stated:

"A number of IMO's web-based services are currently unavailable, including IMO's public website… The interruption of service was caused by a sophisticated cyber-attack against the Organization's IT systems that overcame robust security measures in place. IMO IT technicians

shut down key systems to prevent further damage from the attack. The IMO is working with UN IT and security experts to restore systems as soon as possible, identify the source of the attack, and further enhance security systems to prevent recurrence." Fortunately, the IMO website and public services are now back up and running.

- **CMA CGM's Operations Disrupted by Cyber Attacks**

The French shipping company CMA CGM saw two of its subsidiaries hit with a ransomware attack that caused significant disruptions to IT networks. The Marseille-based shipping giant is the world's fourth-largest container liner by capacity, operating over 200 shipping routes between over 420 ports in over 150 countries. The attack on CMA CGM's two subsidiaries, Mercosul and Containerships, interrupted all of CMA CGM's internal access to its network and computer application because the company sought to isolate the malware and take protective measures. In its latest press release, the company said that its worldwide agency network is gradually being reconnected.

- **Trade & Customs Implications of Cyber Attacks**

Cyber-attacks on the global shipping industry have obvious trade and customs implications. CBP's Customs Trade Partnership Against Terrorism ("CTPAT") is a multi-layered, public/private partnership, which seeks to strengthen international supply chains and improve U.S. border security. The program seeks to closely cooperate with the principal stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers in order to be effective.

CTPAT member companies, or partners, agree to implement certain security procedures throughout their supply chains. To become a partner, the applicant needs to identify vulnerabilities in its supply chain and implement security procedures to safeguard their supply chains from terrorism and other illegal activities that threaten the security of the United States. As a result, the program helps CBP achieve its dual mission of securing the nation's borders while facilitating legitimate trade and travel. In the course of applying, being certified, and thereafter validated, CTPAT applicants/partners are required to submit, via the CTPAT secured portal, business confidential information and sensitive details on how their company adheres to minimum security requirements to join the program.

A key requirement of the CTPAT program is meeting the Minimum-Security Criteria ("MSC"). The criteria were updated for the first time in 2019 since their inception in 2001. The new MSC structure includes cybersecurity as a key focus area, alongside 'security vision and responsibility' and 'agricultural security.'

CTPAT members enjoy benefits such as a reduced number of CBP examinations, shorter wait times at the border, front of the line inspections, and assignment of a supply chain security specialist to the company. However, CTPAT members can only enjoy these benefits if they continue to meet and maintain the MSC, including cybersecurity obligations. The recent spike in cyber-attacks in the shipping industry underscore the importance of keeping your supply chain's cybersecurity in tip-top shape and continuing to meet CTPAT MSC requirements.

- **Cybersecurity & Sanctions**

Cybersecurity risks present sanction concerns, as well. In an October 1 advisory released by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the office warned the public that:

"…demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business."

The advisory went on to describe how facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. Furthermore, facilitating ransomware payments on behalf of a victim may violate OFAC regulations. This is because U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List, other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).

- **If it Looks Like Spam, It Probably Is**

One of the most effective ways to avoid cyberattacks is to screen emails diligently before you open them. Phishing refers to scams in which scammers use email or text messages to trick you into giving them your personal information. ***If emails look suspicious, then it's probably best not to open those messages***. The Federal Trade Commission offers top tips to recognize and protect yourself from phishing and other attempted cyberattacks.

California Cybersecurity Integration Center, By Paul Martin, USCG, 07DEC2020

The California Cybersecurity Integration Center (Cal-CSIC) was established by an act of the legislature in 2015. In 2018, the governor signed a bill supporting a statewide cybersecurity strategy, which further defines the structure and mission of Cal-SCIC as:

"The California Cybersecurity Integration Center shall serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations.

The California Cybersecurity Integration Center shall operate in close coordination with the California State Threat Assessment System and the United States Department of Homeland Security — National Cybersecurity and Communications Integration Center, including sharing cyber threat information that is received from utilities, academic institutions, private companies, and other appropriate sources.

The California Cybersecurity Integration Center shall develop a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices. The cybersecurity

strategy shall be developed to improve how cyber threats are identified, understood, and shared in order to reduce threats to the California government, businesses, and consumers. The strategy shall also strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education."

From Cal-OES Website, 07DEC2020

Cal-CSIC is comprised of several strategic partners, the California Governor's Office of Emergency Services, the California Department of Technology, the California Military Department, and the California Highway Patrol. Additional partners include other Federal, State, and private sector partners including the Federal Bureau of Investigation (FBI) and the United States Department of Homeland Security (DHS). Each partner provides experts to the Cal-CSIC, which serves as the central organizing hub of the State's cybersecurity activities.

The Cal-CSIC is co-located with the California State Threat Assessment Center (STAC), which serves as the State's primary fusion center with the responsibility to protect the State from terrorist and other physical threats. With its core partners, the Cal-CSIC has established multiple capabilities to accomplish its mission:

- **Cyber Incident Response Coordination**

The California Cybersecurity Integration Center shall establish a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state.

- This team shall also assist law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government.
- This team shall be comprised of personnel from agencies, departments, and organizations represented in the California Cybersecurity Integration Center.

- **Information Sharing**

Information sharing by the California Cybersecurity Integration Center shall be conducted in a manner that protects the privacy and civil liberties of individuals, safeguards sensitive information, preserves business confidentiality, and enables public officials to detect, investigate, respond to, and prevent cyber-attacks that threaten public health and safety, economic stability, and national security.

- Cyber Threat Alerts and Advisories

Enables the Cal-CSIC to serve as a conduit for cybersecurity threat information between Federal, State, Local, and Tribal government entities. Advisories and Alerts are also shared with Private sector partners.

- California Automated Indicator Exchange

Provides the exchange of intelligence-driven cyber threat indicators between the Cal-CSIC cyber

threat feeds and partner entities at machine speed, resulting in the distribution of relevant and timely cyber threat and trend information.

- **Phishing Email/Malware Analysis**

Cal-CSIC Analysts collect and analyze phishing emails to extrapolate relevant information about the attacker and their respective tactics, called Indicators of Compromise. These IOCs are added to the California Automated Indicator Exchange to ensure timely distribution to partner entities.

HOW YOU CAN HELP PROTECT CALIFORNIA

State, local, and tribal governments, non-governmental organizations and the private sector can partner with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

- Email the Cal-CSIC to learn more about sharing of IOCs and connecting to the California Automated Indicator Exchange at calcsic@caloes.ca.gov.
- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report suspicious activities or breaches of security to the Coast Guard's National Response Center (NRC), or **cyber-attacks** to the National Cybersecurity and Communications Integration Center (NCCIC):

- (NRC) Phone 1-800-424-8802 or direct phone line at 202-372-2428
- (NRC) Fax 202-372-2920
- (NRC) Web: http://www.nrc.uscg.mil/
- (NCCIC) at 888-282-0870

After calling the NRC/NCCIC, call the Captain of the Port, San Francisco, at 415-399-3530.

Other agencies you may want to consider reporting to are:

California Cybersecurity Integration Center – (916) 636-2997 and CalCSIC@caloes.ca.gov

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- InfraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

CUSTOMER FEEDBACK

How are we doing? Please send feedback about this newsletter to Mr. Paul Martin, USCG Sector San Francisco, at:

- E-mail – Paul.R.Martin@uscg.mil

Note: articles appearing in this newsletter were submitted by port stakeholders or downloaded from public websites and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.