NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
April 2022 (Edition 2022-04)

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 Communications and 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

- **The Cyber Incident Reporting for Critical Infrastructure Act is Here. Now What? –** CIRCIA passed 15 March 2022 – requires critical infrastructure companies to report cybersecurity incidents or ransom payments to the federal government.
- **Are You Mitigating Maritime Cybersecurity Risks?** – Risks and strategies of cyberattacks on ships.
- **Cybersecurity for the Increasingly Connected Ship** – Smarter and connected ships as targets for cyberattacks.
- **Cybersecurity and automation in shipping** – Risks with autonomous ships.

MAIN ARTICLES

The Cyber Incident Reporting for Critical Infrastructure Act is Here. Now What?
Chris Jones, 29 MAR 2022

Earlier this month, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act. The purpose of the Act is to facilitate the hardening of the defenses of key U.S. infrastructure against cyber attacks. As the Act's name suggests, it aims to fulfill this purpose primarily by establishing various reporting requirements, rather than by mandating any particular cybersecurity controls.

What Does the Act Do?
The Act requires that covered "critical infrastructure companies" must deliver a report within 72 hours of certain cyber incidents to the National Cybersecurity and Infrastructure Security Agency (CISA). Those same companies are also required to file a report with CISA within 24 hours of making a ransomware payment. The covered entity may produce the required reports itself, or may instead engage a third party such as an incident response company or law firm. Information reported to CISA under the Act is exempted from the Freedom of Information Act (and state counterparts) and is protected from discovery in litigation and from use at trial.

CISA, in turn, will "receive, aggregate, analyze, and secure" these reports in order "to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls." CISA will share its information and analysis with government and private stakeholders, including actionable recommendations on ways in which to identify and mitigate the threat from known cyber exploits. At a minimum, this reporting will include quarterly unclassified reports available to the public, as well as monthly briefings of congressional leadership and relevant committees. The information contained in these reports will be anonymized.

What Remains to be Done?
Quite a bit. The Act leaves many details to be filled in through the rulemaking process. For instance, the Act does not define which entities are considered "critical infrastructure companies" covered by the Act, nor does it define the type of cyber event that triggers reporting requirements. CISA will also have to develop principals guiding its determination of how and when to share information, what type of information to share, and with whom. CISA is not required to issue proposed rules for two more years, and is not required to issue final rules until another 18 months after that.

What Does the Act Mean for You?
Entities likely to be considered "critical infrastructure companies" should engage with the rulemaking process to ensure that their operational requirements are taken into consideration. At

the same time, they must review their own controls and procedures — particularly incident response plans — to ensure they are able to meet the Act's reporting requirements.

The Act also has implications for entities unlikely to be considered "critical infrastructure companies." Bad actors more interested in money than geopolitics often choose victims they think will offer the least resistance. The Act will provide valuable information that can help any entity better understand and react to the threat landscape. Those that don't act on this information and harden their defenses will become softer targets relative to their peers, and are more likely to attract the unwanted attention of cyber criminals.

Are You Mitigating Maritime Cybersecurity Risks? Dennis Scimeca, 09 FEB 2021

The maritime industry transports 90% of the world's trade and cyberattacks on shipping increased 900% between 2017 and 2020, to the tune of one incident on a ship every day. How much of your supply chain runs across the ocean?

Maritime shipping has proven a juicy target for bad actors in recent years. APM-Maersk in late June 2017, suffered $300 million in losses owing to critical systems infected by malware. China Ocean Shipping Company (COSCO) in July 2018, shut down its American IT network to prevent the spread of a ransomware attack.

In April 2020, Mediterranean Shipping Company (MSC) suffered a cyberattack on servers at its headquarters in Geneva, Switzerland, forcing a five-day website shutdown that prevented customers from making bookings through the portal. A ransomware attack against CMA CGM, the giant French maritime transport and logistics company, in September 2020, forced the company to shut down part of its network.

In a more recent incident, on November 25, 2021, Swire Pacific Offshore (SPO), the maritime services division of the Swire conglomerate, issued a notice that it had fallen victim to a cyberattack, resulting in authorized access to IT systems and loss of confidential, proprietary commercial information and personal data. The CL0P ransomware group later claimed responsivity for the hack, a claim deemed credible by BleepingComputer after viewing some of the stolen data, that included bank details and passport scans.

"The disruption of ships, ports, communications and shipping lanes is a genuine threat. This is crippling to the larger economy/larger supply chains—especially with things stretched thin today," says Steve Moore, chief security strategist at Exabeam. "Amazon is even building its fleet with its own technology to control these problems more effectively."

Reshoring initiatives notwithstanding, it's tough to imagine either an immediate future where these sorts of attacks do not remain commonplace or maritime shipping no longer represents

such an important aspect of the supply chain. And, some maritime cybersecurity concerns continue to remain almost completely unaddressed.

Three Maritime Cybersecurity Risk Categories

Josh Lospinoso, CEO and co-founder of Shift5, says cybersecurity vulnerabilities on a ship break down into three categories or "flavors" of technology: traditional computer systems, industrial control systems and the communications protocols that control the most critical functions on a ship.

Multiple radio frequency interactions for global positioning systems (GPS) or automatic identification system (AIS) take place while a ship travels. Those signals are not encrypted, creating opportunities for "spoofing," when cyberattackers feed fake coordinates to a ship at sea. Radios on a ship can also connect to critical subsystems responsible for controlling propellers, rudders and generators.

While at port, connections to shore-based networks take place. If those networks are not secure, they make ship systems vulnerable to attack. "Of the four likely [maritime cyberattacks], on the mind—CMA CGM, Maersk, Mediterranean Shipping, and COSCO—three were confirmed ransomware back on the shore," Moore says. "This jams up bookings, scheduling, delivery, etc. and is the most common attack."

Every laptop, storage device and new piece of hardware plugged into the ship's network represents a potential risk. "We've seen ships and aircraft where you've got floppy disks and compact flash drives that get swapped in and out and there's oftentimes poor inventory management, no security around the updates that are flowing off of those systems," Lospinoso says.

The kinds of IT cybersecurity products businesses use for desktop PCs or servers can mitigate some of these threats, especially where in-port connections or hardware interactions are concerned. Nonetheless, "It leaves you with a kind of a scary picture, honestly, that all of these different access vectors give attackers a huge surface area to work with," Lospinoso says.

The second category, industrial control systems like PLCs and SCADA systems, require specialized attention. "There's a whole multi-billion-dollar industry that's grown up there, companies that focus on defending those sorts of assets," Lospinoso says. "These companies are distinct from other sorts of cybersecurity vendors and hyper-focused on this problem because it is unique and different."

It's the third category that concerns Lospinoso the most, the communication standards that connect marine sensors and display units within vessels. GPS receivers, autopilots, wind instruments, depth sounders, navigation instruments, engine instruments, nautical chart plotters, all of these communicate using the NMEA 2000 standard, using OT called a NMEA 2000 bus.

Even with all the preventative cybersecurity a company may install on shipboard or shore-based networks, or the best inventory management for all the various devices that may interact with a ship's computer, one maxim of cybersecurity is to accept that a determined attacker will always find a way in. So what happens if an attack succeeds at gaining access to ship systems and then plants malware inside the NMEA 2000 bus?

"Your GPS receiver could course correct the autopilot that's steering because it's all sort of one big chat room. What happens if there's a nefarious participant on that bus? The answer is very, very bad things," Lospinoso says. "There are virtually no folks that are focused on these serial data networks. This is changing over the past year or two but [still] a huge category of cybersecurity that is waiting to get defined. No one is on the NMEA 2000 bus in a ship, looking to make sure that there isn't some rogue device that's got bad firmware that's taking over that network."

Fight Maritime Cybercrime With Proven Strategies

So what should a company that depends on maritime shipping do in the face of these realizations? First, demand that your logistics partners use proper cybersecurity hygiene at the ports where they weigh anchor. Consider mandating third-party verifications of standards. Make sure your shipper has a solid first line of defense.

Next, acknowledge the existence of this special category of OT on maritime vessels. Just as an IT department can probably do a query within 30 seconds and say what version of the Linux operating system runs on servers, someone should be able to answer a question about what firmware versions run on all of a ship's depth transducers.

Finally, realize that the sorts of IT cybersecurity processes and principles already in place at companies may serve as a template to also monitor the OT assets on ship. Then, take action.

"We haven't adapted those practices and principles and patterns to the ships themselves, to the control planes that run the central nervous system systems of these ships. And that is, to my mind, the biggest latent threat that exists to maritime industry," Lospinoso says. "There's zero observability into those things at a corporate level and those are arguably the most critical components to generating revenue for the business."

Cybersecurity for the Increasingly Connected Ship, Mike McNally, 23 FEB 2022

Ships are becoming smarter and more connected, but the new and exciting opportunities for operational efficiency also bring the increased risk of cyberattack. There is actually no way for a ship's network to 'know' its level of cyber resilience, even though a 2020 BIMCO/Safety at Sea survey saw respondents highlight this as significant: 77 percent said they would cancel a contract if they had concerns over cyber security measures in place.

However, effective segregation of systems and access based on need and authorisation can provide a strong basis for successful cyber risk strategies. The multi-layered approach can significantly impede an attacker's access to a ship's systems, while also preventing the spread of malware.

The multi-layered approach

For example, connected OT systems onboard should have more than one technical and/or procedural protection measure. Perimeter defences such as firewalls can prevent unwelcomed entry into systems, but this may not be sufficient to cope with insider threats. In this case safe zones should be considered as a second layer of protection which can be created using firewalls to partition onboard networks and protect confidential data and safety critical systems.

How others are accessing a ship's network is also a key consideration. Virtual Private Networks (VPNs) can offer a further layer of protection by separating crew or third-party traffic from the ship's network. However, resilience depends on VPNs being configured properly and well managed: in some cases, where multiple VPNs are in use, they can actually increase the ship's attack surface and 'punch holes' in its cyber security.

Securing ship networks

These are the considerations which have driven the development of GTMaritime's intelligent data transfer platform, which removes the need for multiple VPNs. It significantly reduces the attack surface using layered security which allows vessel operators to control access to data without opening vessel networks.

Other important considerations to mitigate the cyber incidents include automatic software updates and training. Ensuring all software is up to date is critical. Cybercriminals often look for out-of-date software as the weak link that can provide a route to network infiltration, especially where third-party systems interface with ship networks. One solution is a service that provide fleet-wide updates automatically, anticipating and removing vulnerabilities.

Providing cyber security training to employees is also a key factor in preventing or containing a cyber-event. Seafarers whose contact with the outside world is reliant on the IoT must be especially vigilant regarding phishing emails, clicking malicious links from unknown sources and understand the systems which maintain the vessels cyber integrity. To support crew training, a phishing penetration test allows shipowners to test staff responses to phishing attacks.

An autonomous future

As autonomous ships evolve, they will be more connected and operate within a more extensive cyber-physical infrastructure than even the smartest ships of today. As automation increases, greater efficiencies will be required to support a smaller crew and protect systems as data traffic moving between ship and shore increases.

For example, with less human intervention, unexpected problems may need to be handled remotely, making the resilience of the ship to shore link more critical than ever. There will need to be ample bandwidth and a failsafe system in place in the event that the communications link is broken, or if a remote operation center is hit by a power outage.

With machinery, sensors, systems, and networks interlinked and connected to the internet, any vulnerability in cybersecurity therefore has the potential to become a serious chink in an autonomous ship's armour if not managed properly.

Cybersecurity and automation in shipping, Nir Ayalon, 21 FEB 2022

Covid has taught the shipping world a lot of things. People can work remotely, global supply chains are fragile, and travel restrictions have placed an immense strain on the seafarers that are operating the vessels that keep the supply chains running.

From a human angle, the global travel restrictions put in place have led to crews being stranded onboard vessels, sometimes for over a year, simply because no country would allow crew changes. As a seafarer, there are no evenings, weekends, public holidays or days off when you are signed on. The job is 24/7, 365 days a year.

You know that when you sign onto a vessel but when seafarers remain on the vessels much longer than their original contracts, it is inevitable that fatigue will set in. This increases the risk of human error or poor judgement. The M/V Wakashio running aground and breaking apart in Mauritius is a good example of this. Why was the vessel sailing so close to shore, despite knowing the risks? The crew were trying to get a phone signal so they could call their families.

Shipping lines have been looking at autonomous, or semi-autonomous vessels for years. Crewing is the third largest cost of operating a ship, and the shipping industry is always looking at ways to reduce costs and perhaps Covid is going to be another push towards the goal of reducing the reliance on humans in the operation of ships.

In addition to reducing manning costs, there is less space needed to accommodate crew on ships. Fewer crew equals less accommodation which, in turn, equals more space for carrying cargo.

Autonomous vessels are not a pipedream. It is already possible to have a vessel that is quite capable of navigating itself, avoiding collisions with other vessels and following traffic separation schemes, so why aren't they already widespread?

The recent developments in Machine Learning and remote sensing, with the extensive testing of remote vehicles are bringing this technology closer rapidly. Although we are not quite there for

commercial lines, - there are several autonomous and semi-autonomous vessels already active at sea such as multipurpose USV's (Unmanned Surface Vehicle).

The autonomous ships market size is estimated by Allied Market Research to be valued at $85.84bn in 2020, and is projected to reach $165.61bn by 2030, registering a CAGR of 6.8% from 2020 to 2030.

Where I do see this moving forward are semi-autonomous vessels. The ship handles the mundane and predictable navigation but is monitored from a shore-based operations centre that can take over when needed.

An autonomous or semi-autonomous vessel will follow both the programming it has been given and the data that it is being fed. What happens if that data is compromised? What happens if the vessel is vulnerable to cyberattacks?

A cyberattack, or breach can be as obvious as the vessel losing all control, as we saw in the Gulf of Oman, or as subtle as a minor change in the GPS position of the vessel that isn't immediately apparent, even to an experienced bridge team, such was the case of the Stena Impero.

As this technology develops faster, and legislation begins to catch up with it, cybersecurity is something that needs to be at the forefront of everyone's minds as we move from semi-autonomous to fully autonomous vessels, which is where the industry is naturally going. The entire supply chain is moving towards automation and digitalisation, and in the case of autonomous vessels this also means that operations will no longer be overridden by human intervention, which without proper security will become "floating targets".

James Soon, General Manager of Zycraft USV Pte Ltd said: "Cybersecurity is intricately linked to the unmanned ships. We see these two subjects as twins or two sides of the same coin. Ships may be smartly unmanned, but the confidence in that comes from strong cybersecurity because the unmanned ship owner always wants to know what that vessel is doing. Remote communication is key.

"Here at Zycraft, cybersecurity is front and centre of our vessel hardware design as well as communication design. We engage with capable partners like Cydome to evaluate our cybersecurity approaches and also to harden it. We know that cybersecurity is dynamic and therefore constant watchkeeping is needed."

The one thing we can be sure of in the future is that cyberattacks on the world's maritime fleet will continue and potentially increase. With 90% of the world's economic output being transported by ships every single day the value of criminal or terrorist attack is too great for the threat to disappear. The only way to reduce the threat is to produce better defence and

countermeasures and make cybercrime less rewarding. That is why we reinvest a significant percentage of income into R&D.

There was a time when security measures were primarily "detect and recover", but that failed model is long gone. To be secure in the future the model has to be "detect and block".

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 Communications and 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.