NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
April 2018 (edition 2018-04)

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 news letter 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 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

- **Taking Maritime Cyber Security Seriously** – discusses why cybersecurity threats are real and what rudimentary steps can be taken to help mitigate them.
- **Achieving Cybersecurity on the Water** – discusses LCDR Brandon Link's, U.S. Coast Guard, presentation to the Small Passenger Vessel Association's annual meeting.
- **Cybersecurity in The Maritime Industry, in Piracy and Security News** – discusses reporting cyber-attacks, liability issues and changes in European Union laws, regulations and rules.
- **Cyber Security can no longer be ignored as part of the maritime industry's future** – discusses recent (over the past year) cyber-attacks to the industry and what the future may look like.

- **Hacked at Sea: Concerns Grow over Lax Cybersecurity for Ships, Ports** – discusses recent major hacking incidents, especially MERSK/APM and its implications.

MAIN ARTICLES

Taking Maritime Cyber Security Seriously, MTI Network, 01MAR2018

Despite the recent years' NSA spying revelations, numerous international malware attacks and North Koreas' hacking of Sony Pictures, maritime cyber-security is not an issue at the forefront of many ship-owners and managers minds.

However, whilst the maritime industry might not seem a likely target, reports of successful cyber-attacks are not unknown. Take, for example, the Port of Antwerp, where hackers working with a drug-smuggling gang repeatedly breached digital tracking systems to locate containers holding large quantities of drugs. They then dispatched their own drivers to retrieve the containers ahead of the scheduled collection time. After two years, the operation was eventually shut down and there were no major repercussions for the Port of Antwerp or the companies involved. However, according to security experts at **Trend Micro**, these companies were extremely fortunate. Using the same techniques, it would not be difficult for criminals to cause chaos at sea. By simply accessing and manipulating a vessel's AIS, hackers could prevent ships from providing movement information, cause AIS users to detect vessels in false locations or make "phantom" structures or vessels appear.

Other examples of an industry at risk include a drilling rig being hacked and forced to suspend operations, as well as a container line's entire database of cargo information, including container number, location, place of origin, being erased. Furthermore, instances of maritime and offshore companies that have potentially fallen victim to cyber-attacks may be under-reported, as companies may fear appearing to have allowed confidential information to be compromised. While maritime cyber-security is an issue that falls outside MTI's traditional domain, we are in a position to use our platform to raise awareness of the issues at the executive level. Adopting good "cyber-hygiene" will dissuade opportunistic attacks and prevent accidental security compromises.

Developing and implementing such policies will require a top down approach within a company. At the most basic level a company should:

- Set strong user access controls
- Set strong network access controls
- Perform regular backups
- Keep software up to date

Training employees on how to recognize cyber-attacks and implementing policies on computer hard-ware usage, particularly the use of USB memory sticks, are further steps a company should consider. Doing what you can to secure your networks and taking the time to integrate cyber-security into your risk management and crisis communications procedure, are the two most strategic things you can do to ensure you can respond effectively to maritime cyber-security threats and in doing so, protect your reputation as a secure service provider.

Achieving Cybersecurity on the Water, Jerry Fraser, WORKBOAT, 01FEB2018

If Russia can hack its way into our elections and digital mischief makers in China can deface the White House website, what chance do vessel operators have of maintaining cybersecurity within their fleets? Once we're networked, there probably is no such thing as absolute security, but given our dependence on digital data for everything from navigation to vessel maintenance — to say nothing of life safety — we cannot ignore the need to protect our operations from exploitation or attack.

As part of its mission to promote human safety, marine safety and environmental safety, the U.S. Coast Guard, with the support of the Transportation Security Administration, is leading the charge for cybersecurity in the maritime community. During a presentation Tuesday at the Passenger Vessel Association Annual Meeting at MariTrends in Savannah, Ga., Lt. Cmdr. Brandon Link, a marine safety expert with the Coast Guard's Critical Infrastructure Branch, said the stars are aligning for such an effort by passenger vessel operators, among others. The Coast Guard is developing specific cybersecurity "profiles" for maritime sectors and has completed three, for maritime bulk liquid transfers, offshore operations and passenger vessels. The next profile will focus on navigation and automation.

"The cybersecurity framework profiles are designed to assist organizations in assessing cyber risks and offer guidance on how to allocate limited resources in order to improve their cyber resiliency," Link said. Link said the profiles are designed to facilitate implementation. They leverage existing standards and recommended practices. In the case of passenger operations, for example, the profile was developed in consultation with the Cruise Line Industry Association and the PVA. "We cannot stress enough our appreciation to the stakeholders from all sectors of industry for their assistance in drafting these profiles," he said. Moreover, he said, cost-effectiveness was critical, as was the need to avoid creating a lot of new regulations. "We do hope this is a useful tool," he told PVA attendees.

Cybersecurity in the Maritime Industry, in Piracy and Security News, Shipping Law News, 29JAN2018

The global shipping industry – much like air, road and rail transportation – is undergoing a technological revolution. From hull cleaning to collision avoidance systems, automation has made incredible advances in recent years. There is more to come, too. Norwegian company Yara has partnered with the engineering group Kongsberg with plans to launch the world's first automated container ship in 2018. Rolls-Royce is also joining the fray, having revealed plans in September to build autonomous naval vessels.

There are good reasons for embracing these innovations. For starters, unmanned ships are thought to be potentially safer and more fuel efficient. Automation also frees seafarers from the drudgery of paperwork. But these benefits come at a cost. One of the key challenges in the coming years (and one of the focal topics of BLG's Maritime Law Seminar on December 1, 2017), is how the shipping industry will cope with the growing threat from cyber-attacks. "Ships have an opening to the outside world," Chris South, a senior underwriter for West of England P&I, told the audience present at the seminar in Montréal. "And wherever there is an opening there is a vulnerability."

A recent case in point is shipping company Maersk, which suffered $300 million in damages following a hit by the NotPetya ransomware outbreak in June of 2017. The shipping giant picked up an infection that spread into its global network and was forced to halt operations at dozens of port terminals around the world. "Four factors are at play in the maritime industry", said South. The first is automation itself, as machinery on vessels is increasingly controlled by software. The second is integration. On any given vessel, there may be multiple systems connected together. The third is the ability of ship-to-shore systems that communicate via remote monitoring. "Ships are now talking to head offices continuously," says South. The fourth factor is that all these systems are connected through the internet.

Virtually any company that now relies on these systems is exposed to a cyber cascade of sorts, South added, "where one part of the industry ends up infecting another." So, a shipping company's systems might get infected at headquarters. The infection then spreads to the ship and charterers before moving on to ports and terminals, the logistic companies and ultimately the manufacturing plants receiving the merchandise.

Too big to cover?

The alarming question for insurers in the maritime industry, who view cyber as a growing systemic risk, is "where does the liability stop?" Insurers have voiced concern that the risks are too big for them to cover alone – without government intervention. Understandably, cyber and

data risk insurance is limited when it comes to coverage. “A typical cyber risks policy will cover breach costs, such as forensic investigations, legal advice and those associated with notifying customers and regulators”, said South. It will also cover business interruption; repair and replacement of websites, programs and data caused by hackers; extortion; and the cost to defend and settle claims made for failing to keep customers’ personal data secure. “But it does not substitute or replace the covers lost,” South warned.

New laws on the horizon

One area where governments are stepping in is on the legislative front. Data security breaches are nothing new but gone are the days when organizations could conveniently sweep them under the rug. “Canada is the latest country about to implement a new breach notification regime”, said Éloïse Gratton, a BLG partner and nationally renowned expert in privacy and data protection. Following recent amendments to Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), private-sector organizations doing business in Canada must report the breach to the Privacy Commissioner and, generally, notify customers if there is a risk of significant harm resulting from a data security breach. Gratton expects regulations prescribing the breach notification process in Canada to be in place as early as during the first quarter of 2018.

“There are record-keeping obligations,” she added. “When you have a security incident you’re supposed to keep the data.” The duration of record keeping is still being decided by the Privacy Commissioner but could possibly extend to as long as five years. Organizations that suffer a breach must also be mindful of additional provincial breach notification regimes in Québec, Alberta and British Columbia. Additionally, most states in the U.S. also have breach notification laws on the books.

Another game changer, said Gratton, is the coming into force in May 2018 of the European Union’s General Data Protection Regulation (GDPR), which applies to any processing of personal data, namely its collection, use, disclosure or storage. Under the GDPR, organizations that suffer a breach must notify the relevant national data protection regulator as well as anyone who has been affected, and where the breach is likely to result in high risk to their rights and freedoms. Fines for non-compliance are considerable — up to 4 percent of an organization’s annual worldwide turnover or €20m. The GDPR also creates a right of private action against data controllers and data processors. “Complicating matters further”, Gratton said, “the EU regulation has extra-territorial reach”. It applies to organizations that offer goods and services to European residents or who monitor their behavior, through the use of persistent cookies for instance. That includes businesses based outside of the EU.

How far liability extends will also depend in part on the contractual terms. Contractors are increasingly required to meet cybersecurity standards and can be held liable for damages to a company's systems as a result of a virus or malware introduced by an agent or employee.

Being prepared and mitigating the damage

To safeguard ships from cyber threats, companies should follow International Maritime Organization approved guidelines on cyber risk management, which focus on identifying the systems, data and capabilities that pose a risk to operations, when these are disrupted. To do that, companies must implement risk control processes and have the ability to detect cyber events in a timely manner. They must also be able to back-up and restore systems necessary for shipping operations or services impaired following a cyber event.

To mitigate the damage that can result from a breach, Gratton urges organizations to have a breach incident response plan in place well in advance. "You have to know who your internal core team is, and who your external team is," she said. That includes legal, forensic, PR, and information security experts. It is also advisable, when responding to a breach, to ask legal counsel to retain and deal with cyber forensic experts for the purposes of maintaining solicitor-client privilege. **Source: Borden Ladner Gervais LLP**

Cyber Security can no longer be ignored as part of the maritime industry's future, Ieuan Jones, Ashfords LLP, United Kingdom January 8 2018

This article was first published in the January 2018 edition of Marine & Maritime Gazette.

At the start of 2017 we had an article published on cybersecurity and the present cyber-threats to the marine industry. Now, at the end of the year, we review this again in light of new guidance and current concerns in this area. Back in August, the Government Office for Science published Future of the Sea: Cyber Security, as commissioned by the "Foresight Future of the Sea" Project. Future of the Sea contextualizes the threat to the maritime industry within the UK's National Cyber Security Strategy. Amongst other things it identifies vessels, which contain cyber-physical IT systems, as particularly vulnerable to interference from cyber threats.

Future of the Sea identifies three main areas of attack across the maritime sector: increased connectivity and reliance on digital components; increased levels of autonomous control; and globally accessible navigation systems.

Potential technological developments within the maritime industry merit "special attention", including advances in communication, improved sensing and intelligent and autonomous control systems. These pose challenges within cyber security as they build over existing digital

technologies, allowing broader access to ships and vessels. They also make potential software-dependent weaknesses easier to access for those who wish to exploit them. Recommendations include white collar, "dry" office-based security precautions should be brought better in line with IT systems in other sectors. This is particularly the case with navigation systems, which are so critical to the maritime sector and so have increased vulnerability. Control systems for vessels, offshore units and port systems also need to have attention paid to them. Support from the UK's National Cyber Security Centre (NCSC) is another specific recommendation.

Overall, Future of the Sea imparts an important lesson that, although the marine sector represents a large part of the economy in itself, it should not consider itself a sector in isolation. The marine sector must work with other sectors to shore up its ability to withstand the cyber-security threats to it which will become even more frequent. This will include:

- Knowledge sharing of threats with other industries;
- The introduction and implementation of attack reporting systems;
- Coordinated incident response; and
- Capability development and assurance and compliance regimes for sector adoption.

Last year, the published Guidance on Cyber Security on Board Ships (from BIMCO, CLIA, ICS, Intercargo and Intertanko) was also met with interest. This demonstrates the increasing emphasis that is now being placed on cyber-security as a high priority across the industry. However, what is clearly of concern to parties in the marine sector (shipowners, charterers, insurers, cargo handlers etc.) is the likelihood of legal claims (as well as counter-claims) that may arise when a cyber-security attack happens.

Take, for example, a situation where a guidance system is hacked by pirates in order to implement criminal or terrorist objectives. Much like current scenarios involving the physical takeover of ships, a great deal will turn on a vessel's preparedness to handle a cyber-attack. The vessel's "seaworthiness" should include whether the vessel has an efficient and competent crew and whether sufficient measures are in place on board to meet these challenges. Inevitably, such measures will be decided by reference to the state of knowledge in the industry at the time.
It therefore stands to reason that those in the industry should familiarize themselves immediately with the aforementioned guidance as well. These parties should not only put procedures in place that will limit or, hopefully, eliminate any intended damage from a targeted cyber-attack. Also, in the regrettable circumstance that an attack should prove successful, the party could then prove that, at least, they had the policies and procedures in place to deal with the attack in order to limit its scope.

Cyber risk management systems and protocols, including adequate training for employees - not only at sea but on shore as well - should be put in place to mitigate and avoid cyber-attacks. This will eventually become part of the definition of seaworthiness, as it has already in some quarters.

With each New Year comes new possibilities, as well as new risks. It is important for all parts of the marine sector, from shipowners and other insureds to insurers themselves, to grapple with the size of the threat from cyber-attacks, which are becoming ever more apparent and commonplace.

Hacked at Sea: Concerns Grow Over Lax Cybersecurity for Ships, Ports, Jessica Lever, 05FEB2018.

As hacking risks grow and maritime operations become more digitally connected, experts in industry and government have long said no one is prepared. This summer was a wake-up call. The Port of New York and New Jersey is the largest port on the east coast of the United States, touted by officials as the "gateway to one of the most concentrated and affluent consumer markets in the world." But for a few weeks last summer, the goods moving through one of its terminals slowed to a crawl because of a global cyberattack that originated 4,500 miles away. "The delays were six to eight hours to pick up a container," said Jeffrey Bader, chief executive of the trucking company Golden Carriers, recalling when a terminal in Elizabeth, New Jersey, switched to manual operations while its systems were down. "The line was many, many miles long. Trucks, trucks, trucks."

The terminal's operator, APM Terminals, is a subsidiary of the world's largest container shipping company, A.P. Moller-Maersk Group. The company, which transports roughly 20 percent of the world's cargo containers, was among the hardest hit by the NotPetya ransomware. NotPetya sprouted in hacked accounting software in Ukraine in late June, and by exploiting a weakness in Microsoft Windows operating systems, quickly went global as it infected corporate networks and locked down the data of contaminated computers. Hackers would usually restore access after a ransom payment is made, but NotPetya was engineered to cause chaos more than extort funds, cybersecurity experts say.

Maersk and many other global firms affected, such as FedEx and pharmaceutical giant Merck, were not specific targets of the attack, but that didn't matter. In a "heroic effort" over 10 days, Maersk reinstalled 4,000 servers, 45,000 personal computers and 2,500 applications, Chairman Jim Hagemann Snabe said at the World Economic Forum meeting in Davos last month. Snabe called the episode a "very significant wake-up call" that cost Maersk, which has been applauded for being unusually public about the whole episode, as much as $300 million. The entire shipping and maritime sector, a crucial part of the global economy that impacts ocean health, heard that alarm bell. It is, according to many experts, an industry that is lagging in its preparedness to face modern cybersecurity threats. As ships become more connected to online systems and controlled by software, the risks will only grow.

"This summer is when everybody woke up," then U.S. Federal Maritime Commissioner William Doyle said at the Shipping 2030 North America conference in New York City in November.

Companies, governments and experts have, in fact, been gathering at meetings and conferences for the last several years to talk about cybersecurity risks both at sea and at port. These extend beyond the usual I.T. and business concerns common to any corporation to the industrial, navigational and information systems that, if breached, could pose national security, environment and worker safety risks. Both the International Maritime Organization and the global shipping industry group BIMCO have issued cybersecurity guidelines in the last two years, as have national governments and the U.S. military.

But the shipping sector as a whole has been playing catch-up, and it still has a long way to go. "We are about 20 years behind the ball compared to many industries worldwide," Kate Belmont, a lawyer specialized in maritime cybersecurity issues at the firm Blank Rome in New York City, said at the November conference. The long lifetime of ships and the relatively slow pace at which vessel systems at sea have been connected to the internet, along with the particularly global and interconnected nature of the business, all help to explain why the industry has been slow to grapple with cybersecurity threats.

But cyber-attacks and everyday malware infections are increasingly common. The Port of Los Angeles' executive director recently testified before a congressional homeland security committee that the port's three-year-old Cybersecurity Operations Center is handling an unprecedented 20 million-plus cyber intrusion attempts. A survey conducted by maritime consulting firm Futurenautics found that 40 percent of 5,000 shipboard officers surveyed said they've sailed on a ship they know has been infected with malware, its chief executive KD Adamson said.

Unlike Maersk, most shipping companies are tight-lipped about data breaches. "Attacks have been occurring, but nobody wants to talk about, so a lot of people don't believe they are happening," Belmont said. Ken Munro, who works with the firm Pen Test Partners and conducts what is called "penetration testing" to find cybersecurity vulnerabilities for clients, contrasted the shipping industry with the aviation sector, which he says has deployed anonymous reporting systems for all kinds of situations. In that industry, he said, "an incident is viewed as something you can learn from, not something you should hide."

Although many worst-case scenarios at sea – ranging from a hacker taking control of a vessel's navigation systems or causing a ship to spill its oil, explode or sink – have been shown to be theoretically possible, the list of major publicly known cybersecurity incidents is relatively short and not as dramatic. Over the last few years, cybersecurity specialists have uncovered or demonstrated software vulnerabilities and, just as worrying, human oversights that could allow a cyber intruder to gain access to or control of a variety of ship systems. Among them: the navigational Electronic Chart Display and Information System; a load planning system that balances weight on a containerized ship; or even the voyage data recorder.

One researcher demonstrated at a conference in 2017 how he could quickly take control of a billionaire's super yacht, according to the Guardian. Another showed that a ship's satellite communications system was not only connected to the public internet but used default login credentials (for example, a username like "admin") that could allow anyone relatively easy access.

USB sticks that seafarers still carry and can connect to ship systems are one-way malware can make its way to ships and cause trouble, according to Andy Davis, transport assurance practice director at the cybersecurity consulting firm NCC Group. But while ships used to be isolated and off the grid while at sea, now-common "satcom" boxes can also provide entry for hackers looking for access to a vessel's systems. "Hackers who have a modicum of sense, who can discover these devices on the internet, they can find security flaws in them and compromise ships," said Munro.

It is also still uncommon, he said, for ship technology manufacturers to offer a straightforward way for outside researchers to flag software vulnerabilities or bugs they find. "The manufacturers – they really haven't woken up to security yet," said Munro. "It's going to take them several years to get onboard vessel control systems to a point of security where everyone else is already at." For now, major publicly known targeted attacks have largely involved stealing critical information, not compromising a ship's physical systems. In a 2017 report about an unnamed company, Verizon's cybersecurity team described how pirates hacked into a ship's cargo management system to target valuable crates. In another example, the Port of Antwerp in 2013 reported that smugglers had gained access to data system to make it easier bring drugs through the port.

But it can also be hard to tell whether a cyber incident has even occurred. After the separate collisions of two U.S. Navy destroyers in 2017, speculation that hackers were involved prompted the Navy to include a cyber-attack assessment in one of the cases as part of a larger investigation, according to Foreign Policy. Two experts following the Navy's cyber assessment wrote about why these kinds of forensic investigations are new and difficult. "It is clear that we do not yet have the basic tools to definitively answer the question, 'Were we hacked or did we break it?'" they said.

Another widely discussed episode on the Black Sea this past summer left unanswered questions. The U.S. Maritime Administration issued an advisory that about 20 vessels in the area were reporting interference with their GPS systems that could affect navigation. Outside researchers found patterns of GPS "spoofing," in which a false signal confuses a GPS receiver and could potentially misdirect the ship. While it's well known that it's possible to spoof GPS signals – and

the U.S. government is working to develop a more secure alternative to GPS – there's no definitive answer yet for what happened.

As ships become more controlled by software or, in some cases, even autonomously operated, questions about cybersecurity will become even more important – or may slow down adoption of these kinds of technologies. "Right now, cybersecurity risks haven't been solved at all," said Lars Jensen, founder of the Danish maritime cybersecurity firm CyberKeel, referring to autonomous technologies. At a far more basic level, he says, companies need to do more to train workers and develop more sophisticated strategies to protect critical systems.
As a legal matter, it's now even possible that ship owners could potentially be held accountable if a real disaster strikes because of a cyberattack they could have easily prevented, attorney Belmont said. "The definition of seaworthiness now has changed," she said

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan **must report** cybersecurity suspicious activities or breaches of security to the Coast Guard's **National Response Center (NRC)**:

- Phone 1-800-424-8802 or direct phone line at 202-372-2428
- Fax 202-372-2920
- Web: http://www.nrc.uscg.mil/

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

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
- IngraGard 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 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.