Maritime Cyber Security: Future Implications of Autonomous Shipping

Gwyneth Curry

California State University Maritime Academy

November 28, 2018

Abstract

The technological advances in the last five years has been outstanding. In the shipping industry alone, technology is continuing to advance so much that some believe autonomous shipping for cargo ships will become a reality in less than five years. This will decrease shipping costs, reduce lives lost at sea, and allow for more research of the high seas. The benefits are close to eliminating the consequences of cybersecurity threats and attacks. The industry is not ready for autonomous ships because the cybersecurity of the current industry is not up to par. Billions of dollars could be lost in the transition from manned ships to unmanned. Evaluating the current risks in the industry will help evaluate the future implications of autonomous ships.

Introduction

As the world has adopted new technology, so has the maritime industry. The world has seen so much progress since the first ships set sail centuries ago. From compasses to Global Positioning Systems, much has changed. However, the risks of going to sea are still prevalent and have evolved. Cyber systems aboard ships are becoming a vital part of shipping, and the security risks that come with it are changing rapidly. The maritime industry has a history of not making policy until life or property is lost. For example; the requirement for maintaining adequate lifeboats was not mandatory until after heavy loss of life when the Titanic sank. Cybersecurity is a time-sensitive issue that needs to be addressed and managed before it becomes a global security issue. Developing cybersecurity management policies and implementing systems before an incident could happen could be a huge benefit to companies and our economy. Ships are operated to make money and the saying, “time is money,” applies to shipping like no other industry in the world. Due to the nature of technology, a hacker could be relaxing in their home or local coffee shop and disrupt an entire port in a matter of seconds. Experienced hackers are almost impossible to find. Even if found, a potential hacker could be protected by their country due to international tensions or politics. With all the possibilities of a cyber-attack, ships and their owners should be held responsible for updating and installing security on board their ships.

The rapid development of digital technology has propelled the maritime industry forward with the integration of ships, computers, and networks. With the development of radio for communication, ships can communicate with each other to avoid a collision and make plans for meeting in specific locations. Radar further helped reduce the number of ship collisions after adjustments in training was developed. With the development of global positioning systems,

ships know their position and can confirm their given location with celestial navigation. These advances in navigation tools send their information via radio waves. The newer technology, such as automatic identification systems (AIS) and electronic chart display and information systems (ECDIS), pull data from the radio received technology and display it on a public platform, digitally. These programs are now, more than ever, at risk of being hacked from remote locations and changed without anyone noticing. Everything on ships has a purpose; there is no room for items aboard commercial ships that do not have a purpose. Ships first introduced email systems within the last decade and have been vital to the industry. It is another form of communication between the ship and shore. For example, ships can now communicate with their shipping agent for equipment they may need or food supply information. If there are more pressing matters to discuss, a satellite phone call to the ship can be scheduled between the master and shore personnel. Non-vital and non-time sensitive information that does not need to clutter the older emergency systems aboard ships can now be sent through email. Since ships have evolved, they have removed quite a few positions such as pursers who used to handle all the paperwork and communication between the company and the ship. Now, that communication responsibility is on the captain. With all this technology that is ever evolving on board vessels, more ways to hack and thwart the maritime industry from achieving its goals are prevalent. Ships are carrying tons of goods worth millions and billions of dollars. One malicious email can shut down vital systems aboard ships. Vessel networks are extremely easy to hack and shut down; prevention, maintenance, and recognition of malicious data is the way of the future.

This thesis will discuss the current policies; the programs threatened; case studies of past attacks; and how the industry can use resources already in place to help implement a security plan that evolves with technology improvements over time. In its final pages, it will discuss the

future implications of autonomous ships due to the limited resources and research on the future of autonomous shipping.

Literature Review

The transportation industry is severely lacking in cybersecurity. In June of 2017, Maersk was among several companies to be attacked by a Ukrainian bug called NotPetya (Greenberg, 2018). The ransomware attack caused so much disruption for Maersk and the ports of Los Angeles and Long Beach that they shut down for two days. It is suspected to have come from Russia; however, Russia denies all accusations (Greenberg, 2018). Unfortunately, this is not the first cyber-attack to have threatened the maritime industry. Other mischievous individuals and organizations are becoming smarter and more intelligent in the ways they disrupt the industry and production lines. The transportation industry, more specifically the maritime sector, must begin to invest and improve in cybersecurity for ports, shipping companies, and ships.

Cyber spoofing misleads data received by satellite with incorrect information (Ochin, 2017). Attempting to detect spoofing is getting harder as the spoof becomes more elaborate (Tu, Zhan, Zhang, Zhang, and Jing, 2018). There are possibilities of remotely hacking the ships navigation systems using spoofing and projecting false information via the Automatic Identification System (AIS). This tool gives the speed, location, basic ship description (tanker, passenger, etc.), estimated time of arrival, and destination. Navigation tools that ships heavily rely on such as Electronic Chart Display and Information System (ECDIS), AIS, RADAR, Global Positioning System (GPS), and Voyage Data Recorders (VDR), is not encrypted, so they are incredibly susceptible to any attacks made on the system (Justers, 2018). The game is turning into who can steal the most information for the most substantial price tag (Frodl, 2012).

The cost of fixing cyber-attacks could cost upwards of 300 million dollars, as Maersk saw in June of 2017. Cyber-attack insurance could help with losses from companies solving the cyber-attack on their own. Insurance companies are seeing an increase in cyber-attack insurance applications. This is causing difficulties for insurance underwriters to develop policies that are tangible (Perlroth & Harris, 2014). In some specific cyber insurance policies, insurers offer to cover costs such as legal and crisis management; these are easier to put a price tag on. With more research and more cyber-attacks reported, tangible costs of cyber-attacks can be found (de Vleeschhouwer, 2017).

The US Navy is increasing their security programs due to deadly accidents and huge damages caused by many things but also cyber spoofing (Adams, 2018). In 2011 pirates boarded *Enrico Ievoli*, a commercial ship carrying caustic soda which is a hazardous product used to make paper and pulp. The pirates knew that the *Enrico Ievoli* did not have armed guards and were able to steal the ship right under the watchful eye of various navies in the area looking for piracy attacks. The Pirates received their information from the Italian Mafia who ordered the piracy attack and who was controlling and manipulating AIS with cyber spoofing (Frodl, 2012). In this case, it was creating a ghost ship on navigation tools confusing the seafarers and giving false information about the ships' whereabouts to those watching her. These tools are incredibly necessary to safely navigating a vessel, primarily through high traffic areas such as the Strait of Malacca. The shared data AIS offers is vulnerable and can be taken advantage quite easily (Botunac & Gržan, 2017).

At the end of 2002, the International Maritime Organization (IMO) added a section to the Safety of Life at Sea Convention (SOLAS) which introduced the International Ship and Port Facility Security (ISPS). These actions were different than the usual course of action the IMO

chooses to do in the maritime industry. Most changes will not come about in the maritime industry without significant damage done to property and lives lost. For example, SOLAS came out after the sinking of the Titanic, and the Oil Pollutions Act of 1990 (OPA-90) was introduced after *Exxon Valdes* dumped thousands of barrels of oil into Alaskan waters. The ISPS Code introduced the ships security officer, the chief mate. The chief mate is responsible for the safety of the ship and its crew (ISPS Code, 2018). The IMO met a few days after the Maersk attack to issue a statement urging the development and implementation of cybersecurity (IMO, 2018). It is difficult to implement laws and regulations domestically. It is arguably more challenging to create and enforce laws and regulations internationally and have all parties involved agree and ratify.

The Department for Transportation for the United Kingdom developed a Code of Practice for ship cybersecurity. This Code of Practice was designed for ships while moored, berthed, or underway; throughout the ship's life. The Code of Practice was intended to be read by the ship's senior officers, ship owners and insurers, and anyone operating communication technology (Boyes & Isbell, 2017). In any of these conditions, all programs are still online and running. Berthed ships in a port are typically connected to the ports network to monitor cargo loading or unloading, fueling, or ship repairs, among many other reasons. This program uses human principals and promotes good practice in the field and the office. This Code also recognizes the uniqueness of each ship out in the industry, and it should be noted that ships require individualized plans based on their cargo. The Code of Practice does not set standards or equipment specifics; the practice is to decrease the possibilities for cyber-attacks.

Shipboard Navigation Equipment

Today's ships have a massive network aboard to access basic internet which allows the crew to stay in contact with their family. More importantly, this network is for the professional purpose of the ship. A subcategory of the ship's network is the voyage network, "the purpose of the voyage network is to help navigate the vessel," (Booz, Allen, Hamilton, 2018, pg. 3). The subcategory of the ship's network includes all the navigation equipment such as the Electric Chart Display and Information System (ECDIS), Automatic Identification System (AIS), compass, and voyage data recorder. This network gathers information and processes it from sensors and satellite communication equipment. Once all the information is collected and processed, the crew can use the data to make decisions and navigate the ship safely (Booz, Allen, Hamilton, 2018).

Electronic Chart Displays and Information Systems (ECDIS) are the future of chartless shipping. These amazing machines are capable of so much and are already making seafarers lives easier. One of the major problems with them is how quickly they are affected by cyber bugs and attacks. ECDIS put simply, are charts (paper maps of the ocean) displayed by a computer. With ECIDS, updates to digital charts are made via satellite and updated as soon as data is collected. These provide ships and their crews with the most up to date navigation tools and information. ECDIS is connected to the whole ship system, AIS, RADAR, GPS, ARPA, and much more. A breach in security would likely throw the entire ship offline. The ECDIS is a complex computer that collects data from satellites and many other shipboard systems that are a part of the ships network system. The information collected is then compiled in the ECDIS which then displays real-time information on a digital chart. The ECDIS system is updated on a regular basis, typically once a week. Whereas paper charts are updated on a case by case basis.

ECDIS is particularly vulnerable to hacking because its information can be edited or deleted or worse, give access to the rest of the ship's network (Booz, Allen, Hamilton, 2018). Ships that are completely chartless (meaning no paper charts for navigation) are required to have two completely independent ECDIS on board. Most ships have one ECDIS and paper charts because of the cost.

Automatic Identification Systems (AIS) is required on all self-propelled vessels that travel internationally; vessels equal to or greater than sixty-five feet or have more than 150 passengers onboard (CFR164.46 b1, 2). AIS transmits vessel information such as the vessels current status which could be anchored, underway, or restricted in ability to maneuver. It also transmits the vessels GPS position, speed, maritime mobile service identity (MMSI), the ships name, destination, and estimated time of arrival, as well as other information that other ships in the area or individuals with access to Marine Traffic can view. This tool is mainly used for tracking vessels and assisting in contacting vessels that may be near each other to coordinate collision avoidance (Booz, Allen, Hamilton, 2018). This system is exceptionally vulnerable to hacking such as spoofing a ghost vessel, give false alarms, and impersonating maritime authorities (Booz, Allen, Hamilton, 2018).

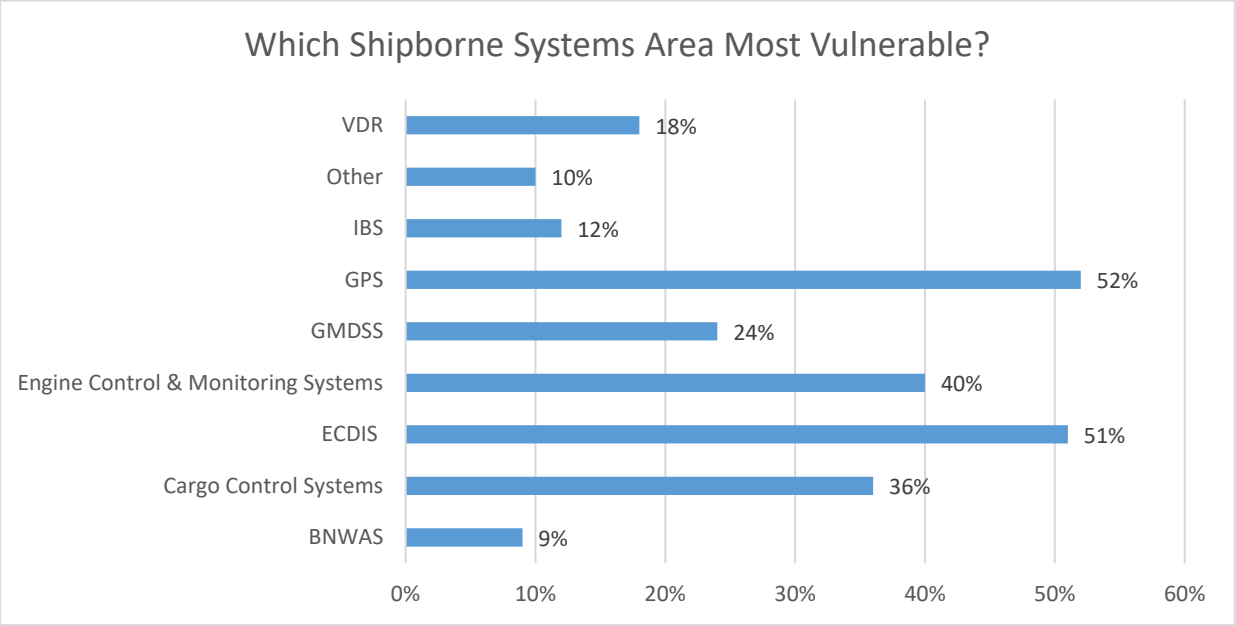
AIS has been a target for hackers since its incorporation to modern shipping. In July 2013, a group of students at the University of Texas was able to hack a ship’s GPS system and falsify its true course and location (Guard, 2017). GPS can be blocked and jammed easily at certain frequencies on transmitters; although this is illegal to do (Booz, Allen, Hamilton, 2018). An engineering network allows the crew to connect to an Industrial Control System (ICS). Which takes the ship's data and assists, for example, an autopilot onboard some ships (Booz, Allen, Hamilton, 2018). The autopilot has access to the ship's rudder and receives information

from the ship's data that is being collected by the navigation equipment onboard (Booz, Allen, Hamilton, 2018).

The United States military maintains and operates the worldwide Global Positioning System (GPS). It is available for public use. However, civilian GPS is strategically less accurate which gives the military a leg up (Booz, Allen, Hamilton, 2018). New and improved GPS are in the making and will dominate the industry with their accuracy and reliability. GPS transmit and receive on certain frequencies that can be jammed or blocked at any time by homemade tools. New networks of digital positioning are popping up around the world to reduce the dependencies the rest of the world has on the U.S. military's system, which is subject to their use and disruption at any time. It is concerning to countries, other than the United States, that the world is at the mercy of the U.S. military and its positioning system. This is the main push towards the development of personal or national specific positioning systems, which is one more thing to improve on.

There are many problems with the current cybersecurity suggestions and proposed policies. The suggestions and policies are broad, have little detail, and not enough content to be effective. One of the biggest vulnerabilities is the shipboard network system. These programs must be reevaluated. Before attempting to fix a hole, the cause of the hole must be identified. To create solutions to cybersecurity aboard ships, an understanding of the equipment's vulnerability is necessary. Too often policy is created by individuals, law makers, that do not understand the basics of the policies up for debate. Many companies still require their officers to take manual fixes by celestial navigation or coastal navigation; should the weather conditions to take these visual fixes exist. However, if a ship were operating about one hundred nautical miles off the coast of California, for example, it might not see a clear sky for a month. In this case, the ship

and its officers must rely solely on their navigation equipment. The major navigational tools that are used aboard ocean-going ships are RADAR/ARPA, ECDIS, GPS or GNSS, and AIS. Below, Figure 1, is a graph based on information provided by Nicola Good in an article discussing a survey taken in 2016. It shows the shipboard navigation systems that are most vulnerable. The category global positioning includes AIS, and it is only behind ECDIS in the ranking of most vulnerable systems aboard ships.



Source: IHS Maritime & Trade © 2016 IHS: 1017218

Figure 1: Created by the author using data from (Good, 2016)

Maritime Cyber Security Survey

A survey of more than three hundred people taken in 2016, showed a surprisingly high number of maritime cybersecurity victims (Good, 2016). Twenty percent of the individuals who responded admitted to being a victim and forty percent of those acknowledged that security programs were in place before the attack (Good, 2016). Of the more than 300 people surveyed, twenty-one percent confirmed company systems targeted, fifty-seven percent had not been

targeted, and unfortunately, twenty-two percent declined to respond (Good, 2016). Below, Figure 2, is a general graph of specific sectors of the maritime industry that responded to the survey.

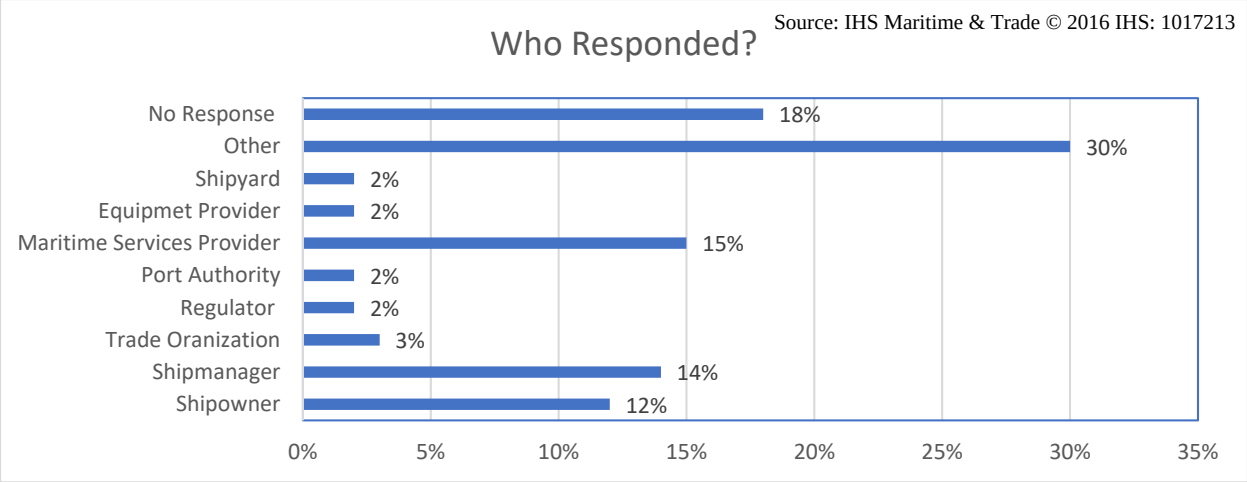


Figure 2: Created by the author using data from (Good, 2016)

There are different categories of cyber-attacks, these are listed below in Figure 3. Out of all the categories, malware is the most prevalent at seventy-seven percent of the attacks (Good, 2016). The second most prevalent form of attack is phishing (Good, 2016). Malware is intended to cause damage and destruction to any system it comes into contact with. There is no point to malware other than to wreak havoc and cause huge losses of data and corruption. Phishing is a form of email hacking by disguising itself as a reliable and safe source that gains secure information if the individual provides. Often, this is how identities, passwords, and credit card numbers are stolen because individuals release their private information on the seemingly reliable page.

In response to the surveys, one respondent admitted that “No one wants to admit the vulnerability of their systems. Ours are based on 1990s-era systems using unsupported Microsoft products (old versions),” (Good, 2016, para. 5). Of the reported attacks, half of the attacks cost less than USD5,000, twenty-five percent had costs upwards of USD 50,000, and two of those

that responded had costs of more than half a million U.S. dollars. This is nowhere near the cost that Maersk endured; it cost the shipping giant over 200 million U.S. dollars. “Half of those who have been a victim detected the attack within 0–6 hours, while 75% detected the attack within 24 hours,” (Good, 2016, para. 10). The sooner an attack is detected, the quicker the system can be recovered and the less damage there is.

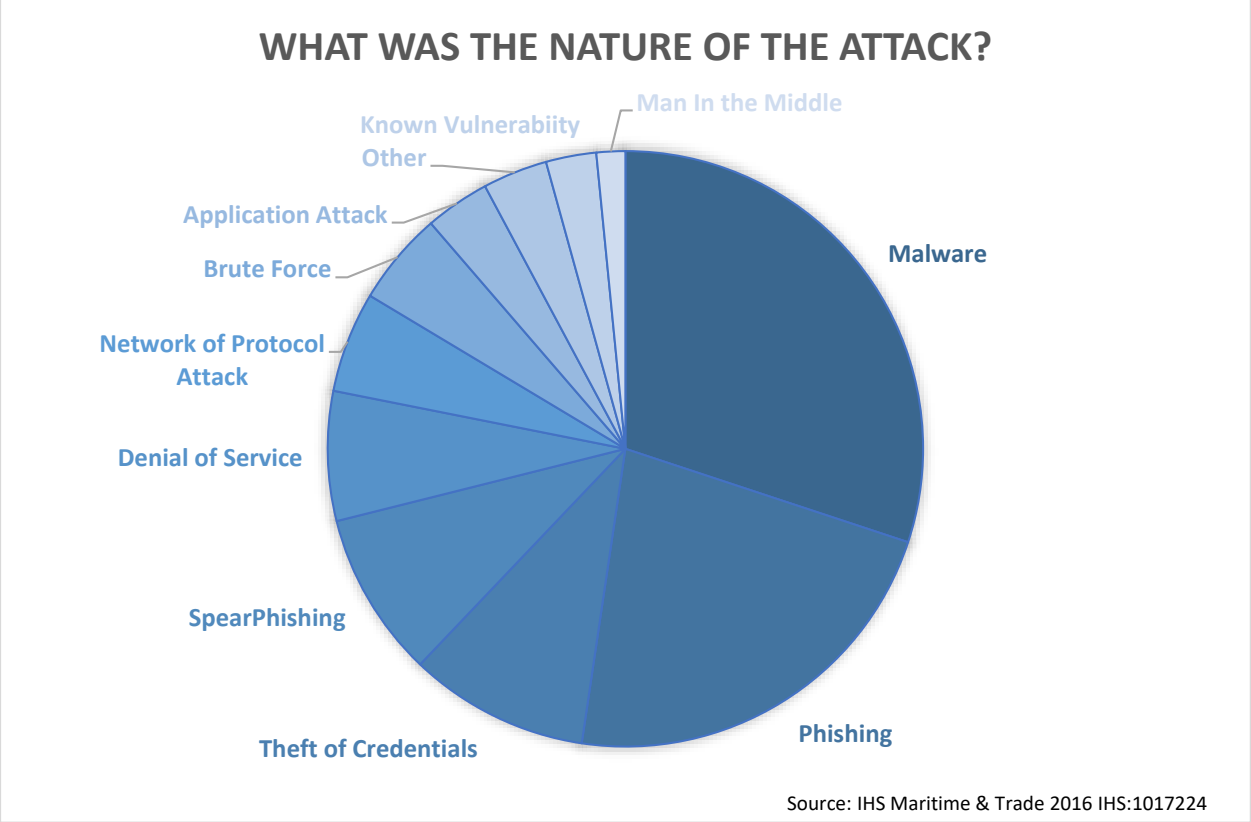


Figure 3: Created by the author using data from (Good, 2016)

Case Study: 2011 *Enrico Ievoli* Pirate Attack

In late December of 2011, the *Enrico Ievoli*, a product tanker, was transiting through the Persian Gulf on her way to the Mediterranean Sea, carrying caustic soda. The location and general description of cargo and crew is public information on AIS, as is most ships operating on the high seas. With a little more digging, the information of the ship such as cargo, crew, and the

fact that there were no armed guards on board, were known to the hackers; in this case, the Italian mafia. This information was given to Somali pirates hired to grab the vessel and hold it hostage with little effort and right under the nose of navies patrolling the area (Frodl, 2012). The hijackers held the crew of eighteen hostages for nearly four months (Schuler, 2012). This was a shock to the maritime community because of the quick transmission of information from one party to the next. It was also a wakeup call on how quickly the pirates were able to seize the ship in such a small amount of time. The pirates are getting smarter and using technology to their advantage.

Maritime industry professionals knew information security was essential to keeping ships more secure and safe back in 2011. Despite this knowledge, pirates were able, and continue to, walk away with more than eighty-one million dollars in 2010 and doubled that amount the next year (Frodl, 2012). If the industry knew that in 2011 pirates walked away with one hundred and sixty million dollars and only returned half of the ships they attacked, there is no excuse for not finding solutions. The pirates are evolving with technology, so the maritime industry should evolve with them and reduce the number of pirate attacks.

In 2017, the industry saw a decrease in piracy attacks with only one hundred and eighty ships being boarded and hijacked. The year before there was slightly more at one hundred and ninety-one attacks (Buneman, Müller, Rusbridge, 2009). This fall is the lowest in more than twenty years. However, in the early months of 2018, those numbers started to rise again; some suggest this is due to complacency (Monks, 2018). Some industry and piracy experts say this is due to navies lack of coordination between counter attacks and prevention (Monks, 2018). Piracy seems to follow a trend; the amount of attacks and rewards reaped from those attacks increase which leads the industry to respond by the presence of armed guard or militaries. The presence

and response of security in these areas leads to a decrease in piracy attacks and rewards. The attacks then increase when the amount of security decreases in pirate infested waters.

Case Study: Maersk June 2017 Cyber Attack

In the summer of 2017, Maersk, a large international shipping cooperation was hacked by an accidental ‘worm’ thought to have come from Russia. Costing upwards of three hundred million dollars, the worm shut down parts of the Port of Los Angeles. This worm is considered an accident because of its nature, the only goal of this worm was to cause damage. This worm is commonly used to compromise tax-accounting software and found a vulnerability in Microsoft Windows systems that relied on a technique stolen from US National Security Agency (Greenberg, 2018). The worm is called NotPetya and attacked other companies during this time, the biggest concern though, is the response or recovery. Much of the equipment aboard ships are run with Microsoft Windows systems. It is important to note that ransomware attacks are described as disruptive and destructive whereas data breaches are specifically designed to go undetected (Cimpanu, 2018). In the case of the Maersk attack, NotPetya was intended to be disruptive and destructive, leaving it classified as a ransomware attack.

Most companies choose not to release this information to prevent more ways to work against their new guards. Maersk is deciding to release this information to collaborate with other companies and to create a platform for the industry, especially shipping companies, to prevent or manage these cyber-attacks and accidents in the future. The hack was such a massive problem because it was not something the company was prepared for. There is no platform or manuals on how to manage this kind of hack; it is all being written as they happen. "There's no benchmark for this," company spokeswoman Katherine Mosquera said. "Is it good? Is it bad? We don't know. It happened," (Leovy, 2017, para 3).

Currently, there are little to no policies regarding cybersecurity aboard ships. Articles about the maritime industry are starting to address cybersecurity issues. The discussion on cybersecurity threats began to make a significant appearance in the early twenty-first century. It is clear now that cybersecurity awareness and prevention did not start soon enough. When think tanks get together, or new technology is being invented, all the consequences of the product or service is discussed and preventions or improvements are found. It is clear that preventative measures were not taken or improved. It is not impossible to imagine a situation like this: "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," (Taking Maritime Cyber Security Seriously, 2018). Or much worse situations by gaining control of the ship remotely and moving the ship and crew to a new location where they can be held for ransom such as the 2011 piracy attack organized by the Italian Mafia.

The attack on Maersk was determined to be an indirect attack; imagine the consequences of a direct attack. Since the NotPetya fell into Maersk's network, the industry is finally starting a serious discussion of future, more direct attacks. So, the threat of a cyber-attack is constantly looming over the heads of every business, individual, and government. The timing of the accidental worm like Maersk's was not as horrible or detrimental as it could have been. Imagine if it had happened during the holidays on a larger scale. Holidays mean may more products being shipped for gifts and deals across the world. As Maersk is one of the leading shipping companies in the world, product delivery could be delayed for months. Companies should never underestimate the magnitude of an attack. The vulnerability must be evaluated, the probability in the future is imminent. It would be a huge misstep to dismiss the large amount of damage a

direct and purposeful cyber-attack could take on any company, especially those on a global scale. Managing the damage and having policies in place is key to recovering from a direct cyber-attack. Limiting consequences from an expected attack is difficult. However, with the correct amount of planning and evaluations, damage can be limited.

Looking at the worst possible damage that can occur, the conclusion is that the damage could be significant. There are think tanks and departments designed and set up for this kind of thinking and evaluations. "…systems are vulnerable to signal loss from deliberate jamming by hackers," Ong Choo Kiat, President of U-Ming Marine Transport (Saul 2017, para 15). On a ship, if the systems are jammed, they will have to return to shore or have another system that can transmit and receive without limitations. "Last year, South Korea said hundreds of fishing vessels had returned early to port after its GPS signals were jammed by North Korea, which denied responsibility," (Saul 2017, para 21).

There are an infinite number of consequences when an attacker is able to hold a company's information and systems hostage. Money, information deleted, or secure information leaked are only a few of the consequences of a successful hack. The hacker can decide how long and how much it requires from the person or company being hacked before they cause more damage. In the worst case, the hacker could choose to destroy all the information they gathered from the victims to teach other companies or individuals a lesson. If companies decide to pay off those responsible for the hacking, they may get hacked again because they will become known for giving the hackers what they want. Once hackers are in, it is easy to hack the same system again. Assuming that a small piece of a virus is not caught while cleaning up, their virus could be left inside for easy access again in the future If companies decide to fix the problem, it may be several times more expensive than the ransom bill. The companies that do not pay the hackers

are less likely to be attacked again. However, they could lose money in the process. Either way, getting hacked can cause significant financial loss.

One way to reduce the financial impact of a cyber-attack is insurance. The key to this is finding an insurance company willing to take on the looming possibility of another attack like Maersk. Not many insurance companies would be willing to take on such a liability. In fact, most insurance companies that cover ships and or its cargo have a Cyber Attack Exclusion Clause (CL 380) (de Vleeschhouwer, 2017). This allows insurance companies to insure the client while releasing themselves from the costs or loss of profit from a cyber-attack. The reasons for excluding cyber-attacks from their policies is because losses from attacks are intangible; there are too many variables to place a price on a cyber-attack. In the survey of maritime cybersecurity, it is important to note that only eleven percent of the more than three hundred individuals surveyed, informed their insurers of the attack. More than eighty percent of the individuals attacked were not covered by their insurance company (Good, 2016). A significant attack on a small or medium sized business could put them out of business. Reporting is a step towards reducing the impacts of cyber-attacks.

Case Study: Fall 2018 Port of San Diego and Port of Barcelona Cybersecurity Attacks

Ports around the world are becoming more prone to attacks; furthermore, the U.S. Department of Defense reports that it "prevents about 36 million cybersecurity attacks," this number represents emails alone (Everett-Haynes, 2018, para 2). The Port of Barcelona and the Port of San Diego were targeted in a cybersecurity attack within two weeks of each other (Cimpanu, 2018). Barcelona was attacked on September 20th, this did not cause a disruption to any ship movements, land operations were affected, specifically the loading and unloading of ships. Later, it was reported that only IT was affected. San Diego was attacked on September

25th, this time it affected more and limited the operations of those working. Unlike Maersk, the two ports are keeping quiet about the attacks and the specific areas that were affected. The ports are also refusing to report the clean-up that is being done to recover from the attack and how the ports of Barcelona and San Diego are planning to prevent another attack. “Shared real-time intelligence on threats would help improve everyone’s defense and vigilance,” (Good, 2016, para. 22).

On November 28th, 2018 two Iranian men were indicted for the attack on the Port of San Diego. The attackers used a malware called SamSam which was used to freeze data and demand a ransom in the form of Bitcon to release the data. This attack was caused by the men who live in Iran. Although the port did not lose its data and no money was given to the attackers, it slowed down the normal operations and caused problems. Thankfully the port invested in strong security practices and backed up all of their systems which allowed them to recover all information. According to the Port of San Diego, it was undergoing updates to its infrastructure during the time of the attack. The question is, what would have happened if the new infrastructure were already in place, it may have prevented the whole attack on the Port of San Diego (Freeman, 2018).

Making a Difference in Maritime Cybersecurity

There are a few companies that are making a difference by evaluating maritime cybersecurity risks. These companies are for-profit and saw a need in the industry and created their businesses based on personal and professional experience. Universities and colleges around the globe are offering classes and research groups to improve cybersecurity not only in the maritime industry but in every aspect of human life. It is evident that the increased use of

cyberspace and technology will only continue to rise. The industry and world must come to an understanding that cybersecurity needs to improve.

MTI Network is a private company striving towards cybersecurity awareness through analyzing incident response reports and managing crisis's before they happen, as they happen, and help with repairing the damages done. The company focuses on energy, shipping, and offshore and transportation industries. Over five hundred incidents, more than three hundred and fifty clients, and about seven thousand vessels are assisted with crisis's all over the world on a yearly basis. These reports in turn help shape future policy put into place working on creating awareness and policies for ships by adopting "cyber-hygiene" (MTI Network, 2018). Cyber-hygiene is similar to at home cyber awareness. Individuals on home networks would not insert thumb drives into their computers because they are like reusing tissues, or not opening unfamiliar emails (Taking Maritime Cyber Security Seriously, 2018). This company helps protect large transportation companies before, during, and after a crisis.

HudsonAnalytix is a maritime cybersecurity analysis company. This company offers a wide range of services based on the client's needs. A small section of what this company offers is boarding ships and evaluating their current cybersecurity technology through a series of inspections and surveys. Their web page has an excellent description of what they do. By starting to address the problems early, potential threats are being eliminated.

> "Those that wait for the IMO to promulgate cyber regulations will be left behind. By the time such regulations are defined, agreed on and propagated via the traditional maritime regulatory bodies the damage done will be far-reaching," (HudsonAnalytix, 2018, pg 1).

While the majority of this company specializes in during and after incidents, a move towards prevention and protection is the company's evolving goal. This is based on client history and the

industry's needs. Navigating the IMO, SOLAS, and countless other regulations set forth by numerous organizations can be confusing and complex, this company offers help with implementing these rules and regulations.

The Department of Homeland Security has developed a grant program for ports looking to expand their security (FEMA, 2017). During evaluations of ports that have applied for this program, it has been found that cybersecurity is lacking. Some evaluations have found that ports are lacking half, if not more, of the cybersecurity protection they should possess (FEMA, 2017). The FBI is also helping combat cyber-attacks. A list of tips can be found on their Cyber Crime web page.

- Employee awareness of ransomware and their roles in protection of the company's data
- Patch systems
- Update antivirus and anti-malware, put on automatic and have regular scans
- Manage privilege accounts, only allow those that are required to have access
    - Read only setting can be useful for shared data
- Disable macro scrips from email
- Backup data on a regular basis as well as the integrity of the backup system
- Be careful of downloading files that are unknown
- Turn off computers when not in use

Good Practice

Seatrade Maritime News published an article in the fall of 2017 on how to enhance cybersecurity on ECDIS; these are extremely raw and basic guidelines. Paul Walters, an ABS director of cybersecurity, was interviewed for the following article. Mr. Walters stated that ECDIS could be taken offline by plugging in a phone into the ECDIS computer port.

Smartphones will connect with most technology to update or back up phone data onto another source. When a phone is plugged into an ECDIS, the ECDIS then goes on a hunt for a way to connect and make contact with the phone to find its purpose. When the ECDIS is unsuccessful and cannot find the phone's connection, the ECDIS will crash. When ECDIS crashes, it is incredibly challenging to reboot or start up the ECDIS due to the large quantity of data on the system. The system is also slow to start up again because the program is of poor quality and rarely updated to keep up with evolving data sent to update the ECDIS.

Ship navigation systems such as ECDIS rely on Extreme Programming (XP). Extreme programming started as a software collection of ideas (Glass, 2001). It is now considered to be the desired way of developing software (Glass, 2001). XP requires the programmer to work with other programmers and software other than its own. It is designed to "capture the functionality or features the customer wants," (Cusumano, 2007, pg 15). Microsoft, unfortunately, does not support extreme programming very well in most shipboard equipment. This lack of support makes systems much more vulnerable to attacks and trips (Hand, 2017).

This article continues to suggest that files downloaded are only placed on to a dedicated thumb drive that is used for nothing else. The dedicated thumb drive should be regularly checked for malware and viruses as well as the computer dedicated to only ECDIS updates. Only after all this is checked and deemed clear of all possible corruptions, then the updated info can be transferred to the ECDIS system (Hand, 2017). This should be standard practice across the maritime industry. "Only 16.8% of ship owner and ship manager survey participants have incorporated cyber-security guidelines into their fleet management systems," (Good, 2016, para. 16).

Code of Practice

The Department for Transportation in the United Kingdom has published a Code of Practice, Cyber Security for Ships. The department recognizes that the maritime industry and its ships are strategically important to the global economy. “Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life,” (Boyes & Isbell, 2017, pg. 5). The Code of Practice states that it is not all about the prevention of hackers penetrating networks, but it is also about regular maintenance and reevaluation of cybersecurity plans. Cybersecurity programs should be designed with strong protective measures against hacks and should be tested regularly. Regular maintenance of programs and plans could result in less damage and disruption if there were an attack. The Code also discusses the importance of being aware and regularly checking for malware and ransomware imbedded in the network. Education to all involved in the industry, including those directly using shipboard tools and programs, will also help prevent cyber-attacks. The more education on cyber awareness, the less mistakes and missteps there will be that could lead to a hole in the prevention system. This practice is intended to be used for the entirety of the ship’s lifespan, as part of a holistic approach to cybersecurity aboard ships.

Developing a cybersecurity assessment starts out with the standards set by the ISPS Code, these should be followed as a minimum. The Code of Practice builds on the standards of the ISPS Code with a ship specific security assessment which is followed by an initial ship security plan. These initial assessments are the ship security cyber and physical evaluations on a large scale. The next steps are to separate the physical and the cybersecurity and dive into the specifics of a cybersecurity assessment. From the initial findings of the assessment, a rough cybersecurity plan can be made. These are evaluated and revisited several times before final

policies and procedures are published. Evaluating risks and creating risk management for threats and attacks is key to a successful cybersecurity plan, see Figure 4 below.

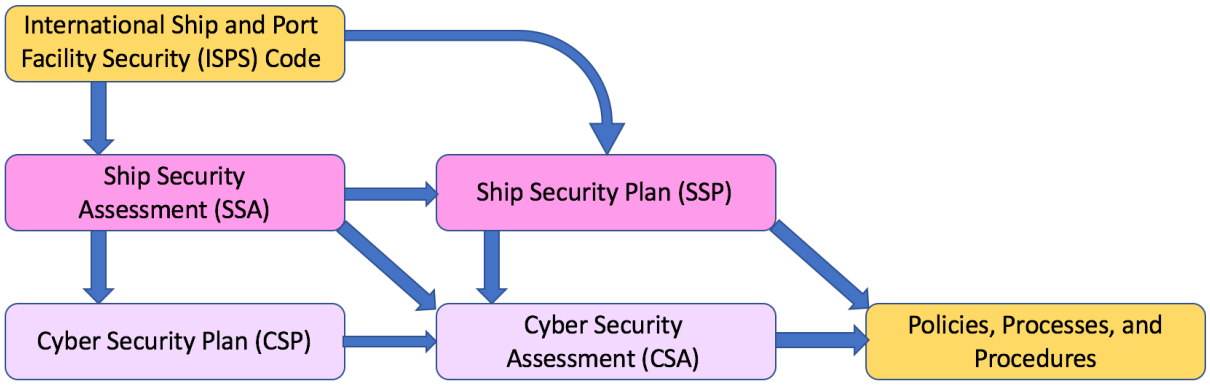


Figure 4: Created by the author using information from (Boyes & Isbell, 2017)

The following are items to target when assessing ship cybersecurity:

- Identify and evaluate vial assets
- Identify and asses the infrastructure the ships business utilizes, understand he internal and external dependencies
- Identify and asses all risks that may present themselves, the probability of risks occurring and the priority of each
- Identify and asses the effectiveness of each security control as well as the costs associated with them
- Identify the overall risk, human factors, all weaknesses, as well as the policies and procedures of each infrastructure

Once the overall cybersecurity plan is complete, it should not be disregarded and placed on the back shelf. The plan should be referenced regularly and reevaluated in an appropriate amount of time. Proactive measures and check-ups should be done regularly to ensure the plans and regulations are followed accordingly. “The CSP (cybersecurity plan) should include a suitable

mechanism for performing periodic, at least annual, reviews of the CSP to verify that it remains fit for purpose," (Boyes & Isbell, 2017, pg. 24).

Adding to the list of personnel associated to the safe keeping of cybersecurity, a Cybersecurity officer (CySO) will be assigned either onboard the ship or a shore-based individual. The CySO is responsible for coordinating and communicating with the company security officer to improve security, develop and maintain the plans and procedures, and implement and exercise the cybersecurity plan. The CySO is also responsible for new laws and regulations that may affect the current cybersecurity plan, especially if the ship operates in foreign waters the jurisdiction of those waters applies to the ship while in those waters.

If an event were to occur, early notification and awareness of the attack is key to reducing the damage inflicted. The security operations center is responsible for the coordination of recovery from an attack. As an event unfolds, it is important to reduce the information leaked, especially sensitive information, to the public or its attackers. This is a way to maintain some control over the situation before fixing or stopping the attack. The Code of Practice developed a flow diagram to assist in the case of a cyber-attack, see Figure 5 below.

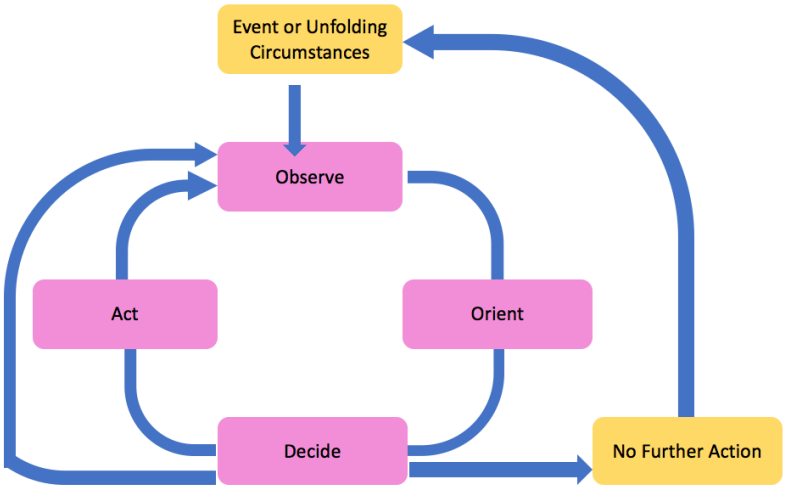


Figure 5: Created by the author using information from (Boyes & Isbell, 2017)

International Maritime Organization

The International Maritime Organization (IMO) sets standards across the maritime industry. The IMO is voluntary participation among the one hundred-and-seventy-four-member states (IMO, 2018). The organization researches, discusses, and votes on international maritime laws that save lives and property as well as the environment. The United States is a member of the IMO and follows a large part of its laws and regulations. There are a few rules and regulations the United States has not signed and ratified because of personal and national conflicts of interests and disagreements. The United States is not the only state to disagree with the IMO laws, regulations, and its member states. Rules and regulations take a significant amount of time to get passed within the IMO because countries have their own national interests and may not want to give up those personal interests. The IMO is also volunteer-based, the members only meet a few times per year to discuss past, current, and future solutions and problems. The main exception to a bill being passed quickly was the Safety of Life at Sea Convention (SOLAS) after the sinking of the HMS Titanic. Unfortunately, the prevailing trend is that bills and laws will not move quickly through the IMO council unless there is a huge tragedy. How could the IMO move the discussion on cybersecurity ahead and focus on getting an answer to help for the ships and their crew?

A new section of the IMO SOLAS Convention is the International Code for the security of Ships and Port Facilities or the International Ship and Port Facility Security (ISPS) Code. This code was adopted in the last month of 2002. The European Union (EU) incorporated the ISPS Code into their laws in 2004. The ISPS Code, put simply, requires ships to have a Ship Security Officer (generally this responsibility lands on the chief mate) which works with the Company

Security Officer. The code should be reviewed, according to the ISPS, every five years. Due to the rapid evolution of technology, this timeline should be more frequent (Boyes & Isbell, 2017).

When Maersk was hit with a malware cyber-attack in June of 2017, it sent a devastating blow to the maritime industry. A few weeks after the incident, the IMO released a Guideline on Maritime Cyber Risk Management. It briefly states that it is highly recommended that companies, organizations, and ship owners invest in their cybersecurity considering the current events. It also states that further instructions and guidelines could be found in their specific government or flag administration requirements, international, and industry best practices. The guidelines note the maritime industry has a dependency on a secure cyber space for smooth operations. However, the IMO urges the industry to make changes to protect its self from potential attacks. They list off specific systems for ships that are vulnerable to attacks: bridge, cargo handling and management, propulsion and machinery and power control systems, access controls, passenger services, passenger public networks, administration and crew data basis, and communication systems. Vulnerabilities in these systems could be from poor design, maintenance, and lack of cyber discipline. Cyber discipline is important and should be considered before downloading files or plugging in a small portable memory drive. It is a broad document with little specifics because the variation in shipping is so huge. These Guidelines are intended for every ship across the industry (IMO, 2017).

Blockchain and Cryptography by Ryan Hoeger

Maritime technology has offered seafarers a faster way to arrive at their destination, find their location, notify shore when in distress, and track ships on their voyage. One skill all mariners should know is celestial navigation, However, this takes time if not practiced regularly. These require calculations of celestial fixes using tables and charts that are in the form of hard

copies on the bridge of a ship. Celestial navigation cannot be hacked, it's all done by hand. Most companies require their employees to log the ship's position every hour on the hour and back up the findings using celestial navigation, weather permitting. When the weather at sea is not permitting a celestial fix, electronic fixes such as global positioning system (GPS) are used. The convenience of digital positioning comes with a price, as they are hackable and can be unreliable.

Building a stronger encryption codes for navigational equipment may reduce the risk of cyber-attacks. These specific pieces of technology make blocking and jamming the information shared much harder for the hacker. Maritime cybersecurity has so much information it would be challenging to cover everything in one paper. Ryan Hoeger, a deck cadet at CSU Maritime, has taken it upon himself to write about these, he is self-taught on blockchain and cryptocurrency. A series of articles on the subject can be found on his Linkedin page.

Blockchains, put simply, are large blocks of data that are grouped together in a sequence of cryptographic numbering systems. For the blockchain to work, they must be in the order of the cryptographic numbering system. The "decentralized, immutable ledger" that Hoeger references are a large blockchain that is mirrored across a network of public and private users if one were to encrypt this access to the blockchain, only authorized users could access the data. The first problem is that their copy of the blockchain key will work on any computer in the network that has access to the lock, or blockchain. The second problem is, with this access, anyone can go in and disrupt or change the data that is available to everyone on a network of computers. Authorized users can go in and change the information which will then balance across the other copies. If an outsider without the key goes into the network to change the data, it won't be recognized, and any changes to the data would not hold. This gets a little more complex when

different keys to access various points in the blockchain access the whole document. Changes can be made at the specific data points a user has so the entire data is not affected, only the part one user has access too. This is especially useful in the maritime industry when different agents at different ports update the status of the goods being shipped (Hoeger, 2018).

Cryptography is incredibly important in today's world to keep information secure. The private key are how information and data is kept private, sharing the private key increases the risk of being hacked and lowers the security of the data. When creating a private account, two keys or sets of numbers are created. "It's how secure text messaging works, it's how private cloud data storage works, it's how blockchain security works," (Hoeger, 2018, para. 2). Encrypted messages are scrambled characters that are protected, to unscramble these characters the public and private keys work together to unlock and unscramble the message. The message cannot be in unlocked without the public and private keys; it would take several million years to unlock with several computers working to unscramble. How the messages are intercepted and decoded is by misplacing or publicizing the private key; therefore, complex passwords and regular changes to passwords are essential and required by some servers. There is only so much one security team can do, consumer participation is essential. That said, private keys are not passwords; passwords give access to private keys and data bases. For example, email accounts are protected by a password, sending emails from the account give access to the private key (Hoeger, 2018).

These series of articles break down the importance of security on one's account and the importance of security in business. Blockchain is important and useful for the maritime industry because it can be used to modify data across a server with multiple individuals with a need to access the data and update it accordingly. Cryptography is a part of the security aspect of blockchain that makes the system nearly unbreakable. How this relates to the industry is by

ensuring private keys are not shared and passwords are complex and updated on a regular basis. When sharing sensitive information about cargo, ship routes, or crew the utmost care to cybersecurity should be made. Below, Figure 6, is a simplified flow map of how encrypted data is processed.

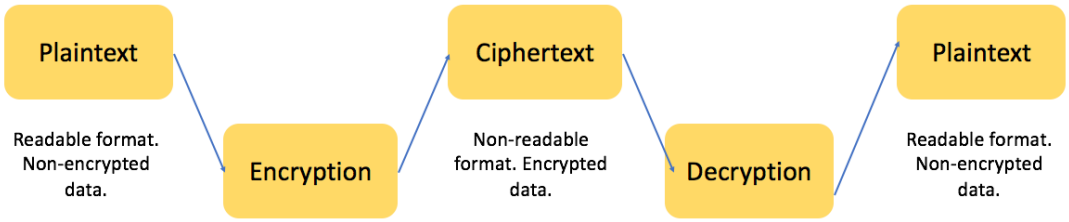


Figure 6: Created by the author using information from (Richards & Pawliw, 2018)

Policy Options: United States Fleet

For shipping, cybersecurity policy is just starting to formulate. If one were to go to congress.gov and type in cybersecurity, a little more than 200 congressional bills appear. If one were to narrow this search to maritime cybersecurity, the search engine pulls up six bills that have only been introduced or passed the house and is still waiting on the rest of the branches to approve. One such bill that was last addressed in November 2017 has only made its way through the House. This bill only contains guidelines and very limited requirements for basic cybersecurity management for ports. Bills are lacking recommendations that could be included to improve cybersecurity. The United States government is only covering a small amount of information that industry experts and all maritime employees should be aware of. U.S. policies should be basic guidelines that companies build on. The second bill was also introduced in November 2017 and it requires an Area Maritime Security Advisory Committee to share information regarding cybersecurity across the industry. This committee would organize the

information and distribute the technology across all parties involved to improve maritime cybersecurity. It would assess the vulnerabilities and identify any areas of weakness for the ships being evaluated. This is a huge step in the right direction, however, is moving slowly through the House because of the lack of research done on the subject. The bill also proposes that security plans be submitted by the operator or owner of the vessel to be evaluated for effectiveness against cybersecurity. These plans would be submitted annually or twice a year, depending on the vulnerability of the ship and its cybersecurity plan.

Policy moves slowly in the United States because of the different political parties constantly clashing and more demanding issues that arise. The slow movement of policy is also due to the constant evolution of technology. There are no way policy makers can keep up with the rapid changes in technology and its ever-growing presence. As a member of the IMO, the United States assists in making laws and regulations and implements the ones they agree with or they sign the whole bill. The likelihood of the United States implementing commercial maritime cybersecurity policies is very small, unless it impacts the government or military. So far, the US has not been affected by a large cyber-attack. In the later part of 2015, Amazon began to investigate Elemental Technologies, a small company that subcontracted to a company called Supermicro to make servers to compress video files for different pieces of technology. Elemental Technologies was a company worth considering because of Amazon Web Services (AWS) involvement in creating a very secured cloud for the CIA that would use Elemental Technologies products (Riley, Robertson, 2018). During the investigation, a small chip, the size of a grain of rice, was found on the motherboard that was not in the original design. Supermicro had the technology manufactured by third parties in China which inserted the microchip into the technology. When news of this broke, it sent a shudder throughout the intelligence community;

especially the U.S. Government who prides themselves on inflicting cyber-attacks (Riley, Robertson, 2018). No consumer information was found to be taken (Riley, Robertson, 2018).

Spies can alter computer systems in two ways; interdiction and seeding the changes at the beginning. Interdiction is the process of manipulating devices while in transit from the manufacturer and the consumer. As the world learned from Edward Snowden, the National Security Association (NSA) favors this approach. China prefers seeding changes from the beginning of a products life. This is what investigators found in the software of products from everyday consumers to top secret level consumers in the U.S. government and military. The Chinese government was able to spy on over thirty companies which included large banks, government contractors, and, the most troubling, Apple Incorporated (Riley, Robertson, 2018). A major problem with this hack is that no one will confirm or deny it, Amazon denies knowing about the manufacturing compromise as well as Apple. No less than six former senior national security officers counter these denials and admit that Apple and Amazon were victims of the hack (Riley, Robertson, 2018). The many moving parts in cyber technology can be hard to track and keep secure. The first step to fixing a problem is to admit there is one. Denial of a problem and the secrecy of being hacked is holding back the maritime industry, as well as every other industry. It seems as if the only people who care about cybersecurity are consumers; they can choose who to do their banking with, their phone company, their internet server, their home security plan, and many others.

Policy Options: International Maritime Organization

Unfortunately, bills take too long to get through the International Maritime Organization (IMO). The key to protecting assists from cyber-attacks is proactive management, some protection is better than none. Often, ship and ports evaluated by private companies such as MTI

Network, severely lack a very basic level of cybersecurity. Getting to the basics of cybersecurity will be a huge step towards global coverage and protection of the world's most important asset, the global trade industry.

Currently, to be a completely chartless ship, the IMO requires that ships must have two completely independent ECDIS systems on board. These must be approved ECDIS systems with regularly updated charts loaded onto the system. Chartless ships are rare aboard brown water vessels due to the costs associated with ECDIS, it is cheaper to update charts manually in the small area the vessels operate in. All officers aboard ships that have ECDIS must be properly trained on how to use them and how to avoid complications and security risks. They also require sufficient backup systems should anything fail. However, despite all this, there are still no guidelines on ECDIS cybersecurity, the industry is still stuck on physical security (IMO, 2018).

The ISPS Code was a significant move in the right direction for security aboard ships. It started out as protections against physical attacks on ships and their ports of call. The ship security officer, port security officer, and company security officers were created as a result of the Code. It specifies the different security levels of a ship while in port and requires different alarm buttons around the ship to notify another party if the ship is being attacked at sea. These are the physical aspects of security. The basic cybersecurity guidelines are to check and ensure all portable memory drives do not contain any viruses or malware before plugging them into a secure computer and to not open suspicious emails. Ships and companies should build from these guidelines to build a specific cybersecurity plan like the Code of Practice made for United Kingdom flagged ships.

The Future of Shipping: Autonomy

Before autonomous shipping starts to make waves and eliminate jobs, cybersecurity for these ships should be evaluated and prevention must be in the forethought of the industries minds. These ships could easily be hacked and lost at sea if precautions are not taken to reduce the likelihood of an autonomous ship accident. Moving technology forward in an industry that has so much impact on the world is important. The fear is that advances are made before the potential threats are thoroughly vetted and protected against. The current focus is building a fully autonomous ship. The mechanics and how these ships will navigate through the oceans on their own is the most exciting aspect of autonomous ships. They will be sending real time data and information to their shore side offices which will make corrections via digital signals back to the ship Thieme & Utne & Haugen, 2018).

The idea of fully autonomous ships is an excellent idea and more research and technological experiments should be done to make it more feasible. The reality of autonomous ships will probably not become feasible for another few decades. The timeline gives the industry time to build up cybersecurity and cyber-attack prevention technology. A survey was presented to the IMOs Maritime Safety Committee (MSC) before they discussed autonomous ships. It reported eighty three percent of the nearly one thousand maritime professionals doubted autonomous ships would enter the maritime industry within two years (Johnson, 2018). Those surveyed also noted that cybersecurity was the biggest obstacle to the autonomous ships (Johnson, 2018).

The MSC started discussing the maritime security of autonomous vessels in May of 2018. The MSC met to initiate the discussion on the safety of these vessels, one of the focus points was piracy and armed robbery (IMO, 2018, para. 19). This is an important aspect that should go hand

in hand with cyber-security of the autonomous vessels that will be controlled via satellite. The IMO Secretary-General Kitack Lim summed up the IMOs stance on the evolving technology of the maritime industry in an interview before the MSC meeting in May. Lim stated that it is important for the IMO be open to the evolving technology that will improve the efficiency of the maritime industry, but also keep in mind the human element of safe navigation to reduce potential accidents (Johnson, 2018).

Analysis

The future of shipping is autonomy and cyber networks. The integration of technology has decreased the need for crew since the beginning of time, it is only a matter of time before ships become totally autonomous. The industry, however, has a reputation of being behind the curve when it comes to adopting new technology. Currently, there are not many major cyber-attacks or hacks. The attacks will continue to increase; however, preventative measures can be made with proper investments in research and development towards cybersecurity. New companies are coming up with cybersecurity solutions, which are providing a step in the right direction. Shipping is a huge part of our industry and will only continue to grow. So far, the attacks on shipboard equipment are small and mainly due to human error and complacency. The attack made on the *Enrico Ievoli* was an initial example of how shore based data can get to ships. The possibilities of total losses to ship power is not all that far off to imagine. Cybersecurity across the world in all aspects of life are still a major problem. Adding ships carrying billions of dollars into the mix seems like a risk that should not be done until the current cybersecurity problems are addressed. Insurance companies are already diligent when insuring maritime risks, they are even more protective and less likely to write policies for cyber-attacks. The likelihood of insurers covering autonomous ships is very small. Not one insurance company would be willing

to take on such a huge loss, there would need to be multiple companies involved in taking a section of the policy. If autonomous ships were to work out, there could be significant profits and benefits to supporting this part of the industry. Even if cybersecurity was not an issue, the transition between manned ships and unmanned ships would be rough because the human element would still exist. Collisions could increase significantly during this time-period. The transition will see a rewrite to ship construction, rules of the sea, and possibly an increase in research collected from the high seas. The other problems are how ships will dock and undock themselves, they could easily be seized just a few days before entering a port.

The common theme continues to be that no one wants to admit that their systems and servers are out of date, the vulnerability, or how they plan on fixing their systems and getting their company back on line. The first step to solving a problem is by admitting that there is one, with more awareness comes more research to prevent attacks from happening.

As technology advances and more navies patrol pirate-infested waters, the pirates have had to attack their victims in smarter ways. The AIS system has become a tool for the pirates and have allowed them to surprise their targets with little notice of the navies patrolling the area. The pirates and those that order the attacks can pick up on details of ships that are left on cyberspace with no protection. This is concerning, commercial vessels and their crew should be protected at all costs. Information of vessels and their specific cargo and crew should never be available for public consumption. This is especially concerning for Western ship's crew, Westerners are considered higher value. Pirates will seek out high value crew over the ships and its cargo. Locking up information and not sharing ship information is a start to making the ships and their companies more secure (Frodl, 2012). AIS should be reevaluated and revamped to restrict access to sensitive ship information.

Recommendations

As shipping is a global trade industry, answers must be given to these questions society has been asking for quite some time: Who is attacking me, why are they attacking me, where is the attack coming from, what could be damaged, what will be attacked (Hudson, Bobys, 2018). "…maritime cyber-security is not an issue at the forefront of many ship-owners and manager's minds," (MTI, 2018). This needs to change before policy is going to be created. Maersk, while an unfortunate event, was a wake-up call to an industry that really needed it. Companies that followed the disruptions and loss the company suffered would bring attention to the risks of cybersecurity to the international community would be the first step, education awareness and consequences of cybersecurity attacks.

Hiring companies such as HudsonAnalytix to survey ships would be a step in the right direction. They not only survey ships but they also survey ports and shipping companies. There is many more maritime cybersecurity think tanks out there. Creating more companies to tackle this international issue would create competition and push changes to happen sooner and become more advanced. The International Maritime Organization is another great organization to start petitioning for more cybersecurity regulations and requirements for ships. Unfortunately, policies move slowly due to conflicts and ever-changing technology. IMO policies and requirements will be created and enforced in time.

Cybersecurity is an area that the world cannot continue to ignore. On a global scale, this is a war against everyone and a war against no one. The world saw what one mistaken "worm" could do to a globally influential company such as Maersk. There are precautions and programs for sale to ordinary people that want to protect their personal lives, the same should be done to shipping companies, ports, and ships. A new challenge that will force cybersecurity into the

limelight is self-driving ships, this will bring a whole new set of challenges and policies. However, the maritime industry must be ready for this, policies cannot be created overnight, and a head start on human operated ships with basic cybersecurity would be a help. Companies should, at the very minimum, enforce stronger user access controls, strong network access controls, perform regular backups, and keep software up to date (MTI, 2018). These recommendations should be the bare minimum standards put in place onboard every ship.

The response time from when an accident occurs to the first person on the scene is prolonged. Slow responses are due to the large surface area of the ocean as well as the restrictions of resources and time. However, management of public and private domains or servers can quicken the response time and put a stop to any cyber-attack from shore. This can increase the security of ships and can be completed in a timely manner with the proper responses and quick action. The maritime industry is notorious for not managing damages quickly enough and having too slow of a response time. Waiting until people are injured or dead, or property and money are lost is not the best response. As the world saw with Maersk, the actions taken to start damage control took far too long after the company was hacked. A policy was written after the attack and the quick thinking, and correct judgment calls were expanded and written into guidelines for future cyber-attacks. Industry experts must be proactive when it comes to possible threats to the maritime industry because it is vital to the global economy. Assessing the damage done, the potential dangers, the risks individuals take in everyday transactions must be considered before moving operations onto a cloud or a system with cloud access. For example, some people still choose to do their taxes and financial information on a digitized system that is not connected to the cloud in any for security reasons. The risk is too significant for them to bear, so they don’t put themselves in that situation. With large volume shipping companies, such as

Maersk, an off-line system is not practical because they operate globally and must use the cloud for easy access of information and efficiency. The risk Maersk took was chosen after careful consideration of all the threats and consequences except for cybersecurity's and vulnerabilities. This is, unfortunately, very common throughout the maritime world.

First, risks must be evaluated at all levels of a shipping company to boil down cybersecurity needed aboard ships. A risk is a cross product of threats, vulnerability, and consequences. One of the main reason's cybersecurity is not the main priority of shipping companies is because it is a relatively new topic. It is only within the last decade that cybersecurity was even talked about. Why anyone has a reason to disrupt or cause damage to a ship or shipping company through cyber-attacks, is the question that should be asked. How much damage are shipping companies willing to risk before they begin to implement prevention and management.

Works Cited

Adams, R. (2018). High-Sea Hacking? *Military Technology,42*(2), 40-41. Retrieved September 17, 2018.

Booz, Allen, & Hamilton. (2017). Introduction to Squarespace. *The Definitive Guide to Squarespace,* 1-26. doi:10.1007/978-1-4842-2937-8_1

Botunac, I., & Gržan, M. (2017). *Analysis of Software Threats to the Automatic Identification System*. Brodogradnja, 68(1), 97–105. https://doi.org/10.21278/brod68106

Boyes, H., & Isbell, R. (2017). *Code of Practice Cyber Security for Ships*. Department for Transport. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

Buneman, P., Müller, H., & Rusbridge, C. (2009). Curating the CIA World Factbook. *International Journal of Digital Curation,4*(3), 29-43. doi:10.2218/ijdc.v4i3.126

Cimpanu, C. (2018, November 21). Port of San Diego suffers cyber-attack, second port in a week after Barcelona. Retrieved from https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/

Code of Federal Regulations (CFR). *AIS Requirements.* Tittle 33 CFR164.46 b1, 2. Retrieved from https://www.navcen.uscg.gov/?pageName=AISRequirementsRev

Cusumano, M. A. (2007). Extreme Programming Compared with Microsoft-Style Iterative Development. Communications of the ACM, 50(10), 15–18. https://doi.org/10.1145/1290958.1290979

de Vleeschhouwer, S. (2017, April). Safety of data the risks of cyber security in the maritime

sector. Retrieved from https://maritimetechnology.nl/media/NMT_Safety-of-data-The-risks-of-cyber-security-in-the-maritime-sector.pdf

Everett-Haynes, L. (2018, October 2). Not on Our Watch. Retrieved from http://newscenter.sdsu.edu/sdsu_newscenter/news_story.aspx?sid=77393 http://www.gard.no/Content/21112216/CyberSecurity

FBI. Cyber Crime. (2018, September 26). Retrieved from https://www.fbi.gov/investigate/cyber

FEMA. Fiscal Year 2017 Port Security Grant Program. (2017). Retrieved from https://www.fema.gov/fiscal-year-2017-port-security-grant-program

Freeman, M. (2018, November 29). 2 Iranian men indicted for ransomware cyberattacks on U.S. targets, including Port of San Diego. Retrieved from https://www.sandiegouniontribune.com/business/technology/sd-fi-charges-port-of-san-diego-ransomware-20181128-story.html

Frodl, M. G. (2012). Pirates Exploiting Cybersecurity Weaknesses in Maritime Industry. *National Defence*,(702), 33-35. Retrieved September 17, 2018, from http://www.ndia.org

Glass, R. L. (2001). Extreme programming: The good, the bad, and the bottom line.IEEE Software, 18(6), 112-112, 111. doi:http://dx.doi.org.ezproxy.csum.edu:2048/10.1109/MS.2001.965816

Good, N. (2016, September 19). IHS Fairplay Maritime Cyber-security Survey – the results. Retrieved from https://fairplay.ihs.com/article/4275151/ihs-fairplay-maritime-cyber-security-survey-the-results

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating*

Cyberattack in History. Wired. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hand, M. (2017, November 17). Simple steps to improve cyber security on ECDIS. *Sea Trade Maritime News.* Retrieved from http://www.seatrade-maritime.com/news/americas/simple-ways-to-improve-cyber-security-on-ecdis.html

International Maritime Organization. (2018, May). MSC-99th-session MSC 99th session //. Retrieved from http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-99th-session.aspx

International Maritime Organization. (2017, July 5). MSC-FAL.1/Circ.3. Guidelines On Maritime Cyber Risk Management. Retrieved from: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

International Maritime Organization. (2018). Solas-X-2 ISPS Code //. Retrieved from http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2 isps code.aspx

International Maritime Organization. (2017, June 16). *Resolution MSC.428(98) Maritime Cyber Risk Management In Safety Management Systems.* Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf

International Ship and Port Facility Code (ISPS Code). (2014). *Maritime ISPS Code Regulations 2014*. Retrieved from http://extwprlegs1.fao.org/docs/pdf/fij152587.pdf

Johnson, B. (2018, May 18). As IMO Weighs Autonomous Ship Rules, Seafarers Warn of Safety Threats. *Homeland Security Today.US.* Retrieved from https://www.hstoday.us/subject-matter-areas/maritime-security/as-imo-weighs-autonomous-ship-rules-seafarers-warn-safety-threats/

Justers, W. (2018). *Proteus Risk Solutions*. Cyber Security at Sea, [PowerPoint slide 5]. Retrieved from: http://www.bvz-abdm.be/sites/default/files/walter_justers_-_cyber_security_-_proteus_presentation.pdf

Leovy, J. (2017, August 17*). Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks*. Los Angeles Times. Retrieved from http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

Monks, K. (2018, January 03). Piracy threat returns to African waters. Retrieved from https://www.cnn.com/2017/05/25/africa/piracy-resurgence-somalia/index.html

Ochin, E. (2017). GPS/GNSS spoofing and the real-time single-antenna-based spoofing detection system. *Scientific Journals of The Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej W Szczecinie,123*(52), 145-153. Retrieved from doi:10.17402/256

Perlroth, N., & Harris, E. A. (2014, June 9). *Cyberattack Insurance A Challenge For Business*. New York Times, pp. B1–B7. Retrieved from https://login.ezproxy.csum.edu/login?url=http://search.ebscohost.com.ezproxy.csum.edu:2048/login.aspx?direct=true&db=aph&AN=96380708&site=ehost-live

Richards, K., & Pawliw, B. (2018, September). What is cryptography? - Definition from

WhatIs.com. Retrieved from: https://searchsecurity.techtarget.com/definition/cryptography

Robertson, J., & Riley, M. (2018, October 4). The Big Hack An Investigative Report. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Saul, J. (2017, June 29). Global shipping feels fallout from Maersk cyber attack. Retrieved from https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from maersk-cyber-attack-idUSKBN19K2LE

Schuler, M. (2012, April 23). Somali Pirates Release Italian Tanker Enrico Ievoli and Crew – gCaptain. Retrieved from https://gcaptain.com/somali-pirates-relased-italian/

Taking Maritime Cyber Security Seriously. (2016, May 31). Retrieved February 20, 2018, from http://www.mtinetwork.com/taking-maritime-cyber-security-seriously/

Thieme, C. A., Utne, I. B., & Haugen, S. (2018). Assessing ship risk model applicability to Marine Autonomous Surface Ships. Ocean Engineering, 165, 140–154. https://doi.org/10.1016/j.oceaneng.2018.07.040

Tu, J., Zhan, X., Zhang, X., Zhang, Z., & Jing, S. (2018). Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring. *IET Radar, Sonar & Navigation,12*(9), 1058-1065. doi:10.1049/iet-rsn.2018.5151