NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
April 2019 (edition 2019-4)

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

- **A Summary of Cyber Threats** – a summary of current cybersecurity threats.
- **A Maritime Cybersecurity Website** – information about the Maritime Cybersecurity Center’s website and tools.
- **Cyber Security at Sea** – maritime industry cybersecurity threats and regulatory compliance issues.
- **Cybersecurity in Maritime** – discusses risks to maritime industry and ships.
- **Maritime Cybersecurity using ISPS and ISM Codes** – discusses using the ISPS and ISM coded with respect to cybersecurity.

MAIN ARTICLES

A Summary of Cyber Threats, Paul Martin (USCG), February 1, 2019

This threat summary is based on a variety of sources and highlights the major cybersecurity threats affecting federal, state and local governments and the private sector.

Business Email Compromise (BEC) Scams

BEC is an attempt to deceive organizations to send money or personally identifying information (PII) or to fraudulently use an origination's name to obtain material goods. The emails often originate from compromised, spoofed or fraudulent accounts; which are used to make requests for data and gain funds. The Federal Government reports the worldwide loss since 2013 has been over $12 billion and account for nearly a third of financial losses and data breaches. Among the most frequent breaches/losses are those involving purchase order scams, requests for W-2 data and financial theft scams (spoofing an organization into sending funds to a false account).

Malicious Spam (MALSPAN)

MALSPAM is the distribution of malicious software (malware) through spam email. It is currently the top infiltration vector for malware throughout California. MALSPAM proves to be a consistently effectively, low cost, infiltration method for both opportunistic and strategic cyber-attacks. It uses common social engineering tactics; by tricking the end user with content that implies a sense of urgency, or appearing to originate from a trusted entity.   Once opened, it downloads malware to the (now infected) computer system. A popular method is the use of password protected attachments to both bypass security and trick users into believing the attachment is legitimate.

PHISHING

Phishing is a cyber-attack that attempts to acquire sensitive user information through deception and most often targets login credentials. It provides cyber threat actors (CTA) an effective, simple and low-cost way to attack computer systems. CTA use open source information to strategically craft phishing emails to be used against public/private sector organizations. Cybersecurity monitoring organizations have noted a significant increase is phishing URLs over the past year, using common third-party services such as; PayPal, Dropbox, Google Drive, and Microsoft Office. Successful attacks can result in compromising credentials that are used to gain access to a computer system, steal sensitive data and allow for secondary (targeted) phishing attacks.

Strategically Targeted RANSOMEWARE

Ransomware is highly likely to remain a high impact threat to organizations throughout California. Cybersecurity monitoring organizations have noted a shift in ransomware threat usage from opportunistic to strategic cyber-attacks; thus, showing an overall decrease in this kind of attack volume. Monitoring organizations note that cyber threat actors (CTA) target specific public/private sector organizations and vulnerabilities to maximize ransom payouts. Most of the targeted attacks exploit vulnerabilities in an organization's information technology (IT) architecture after researching the entity or using other types of cyber-attacks. The attack then encrypts data and back-ups to increase the likelihood of the ransom being paid.

Unpatched and Outdated Software

Many organizations continue to use outdated or unpatched system software due to difficulties in updating their system, use of highly specialized legacy systems or operational needs. These systems leave organizations highly susceptible to many types of cyber-attacks. CTAs can use these systems as a means to infect entire public/private sector networks and systems. Vulnerabilities include endpoints running out-of-date software, unpatched servers, and networks with poor security controls. Cybersecurity monitoring organizations have noted these systems have been compromised ransomware, malware, and server message blocking attacks.

Vulnerable End Users

The end user continues to be the most prevalent cybersecurity risk for organizations state (and nation) wide as most of cybersecurity threats target the end user. Social engineering is often facilitated through the use of emails as the most efficient platform. Such attacks trick the end user into opening attachments or clicking on a URL provided in the email. These emails prey upon human behavior (advertisements, fake tech support requests, etc.) to disclose sensitive information or install malicious software.

The chief cyber threat actors continue to be **cyber-criminals**, who compromise IT systems for some kind of financial gain (either direct monetary gain or profiting from the selling of data on the black market). **Hacktivists** are politically, socially or ideologically motivated persons that frequently employ tactics such as; distributed denial of service (DDOS) attacks, threats, and other attacks to effect desired change. The majority of these attacks are against government entities in response to controversial issues/actions. **Web-Defacers** generally select targets of opportunity, preying on vulnerable systems rather than targeting a specific entity. While seaming minor, they indicate critical vulnerabilities within a computer system's cybersecurity architecture. This can indicate a system's vulnerability to more serious issues; such as, a system's server(s) being hijacked for malicious or nefarious purposes, hosting cryptocurrency miners or being used to harvest data or credentials from other systems.

General Recommendations Include

- Good cybersecurity hygiene practices, such as; using up-to-date security software, updating system software regularly and monitoring "log" files for suspicious internet connections.
- Implementation of industry accepted cybersecurity standards and/or guidelines.
- Implementing intrusion detecting systems (IDS) to detect malware, ransomware and other forms of cyber-attacks.

- Use Group Policy to set Windows Firewall rules to restrict communications between client systems.
- Use user credentialing protocols to restrict user access to various parts of your IT system.
- Disable macros that are not digitally signed by management and not needed for business.
- Disable or remove software, protocols, and portals that are not needed for business.
- Preform regular back-ups to limit the impact of data loss and store those files offline.
- Develop a cyber-incident response plan that is well socialized throughout your organization, develop effective partnerships with upstream service providers to make assistance available to you, and if you use a third-party website host, ensure they are using proper cybersecurity protocols.

Maritime Cybersecurity Website, Paul Martin (USCG), March 15, 2019

While I was surfing the net for newsletter articles, I found this website:

https:\\maritimecybersecurity.org

It belongs to "*the Maritime Cybersecurity Center (MCC) which was created as a result of recommendations from the Southeastern New England Defense Industry Alliance (SENEDIA), along with other leaders in public and private sectors, as a dedicated resource focused on supporting the cybersecurity workforce needs. These leaders called attention to the significant risk from willful threats to electronic connectivity and critical functionality, and identified the need for an independent, not-for-profit organization to focus on cybersecurity excellence and readiness. Our independent, 501(c)(3) not-for-profit status provides a foundation for excellence and commitment to growing cybersecurity knowledge, skills, and capabilities, and developing skilled personnel and growth opportunities for our region.*

*The Maritime Cybersecurity Center is the foundation from which we will **ACT**: (1) build **Awareness** of the cybersecurity problem in our population, businesses, industries, and educational institutions; (2) build **Communities of practice** for increasing understanding and dissemination of information among these groups and related interests globally; and (3) develop and ready a knowledgeable cyber workforce through robust **Training** who can identify, avoid and solve cybersecurity problems, and provide a platform for continuous learning and defense in the field of cybersecurity*."

Contact information:

55 John Clarke Road
Middleton, RI 02842

mcc.info@maritimecybersecurity.org

The website appears to have some useful tools including a two-page information technology check sheet with helpful tips (see attached).

Cyber Security at Sea: The Real Threats, David Rider March 10, 2018

The maritime cyber security landscape is a confusing place. On the one hand, you have commercial providers suggesting the risks of everything from a hostile attack on ship's systems which allows the vessel to be remotely controlled by pirates and direct it to a port of their choice, or causing a catastrophic navigation errors, a phishing attack or ransomware on the Master's PC. While on the other, you have sensible people who point out that this notion is nonsense due to the number of fail safes and manual overrides and controls in place. Then there are calmer voices still, who point out that the most likely threat is actually to the servers inside your head office, or a man in the middle attack on your company's bank accounts.

Recognizing the threats

So, what are the real, documented, current threats to the shipping industry from cyber criminals? Here, we hope to offer some genuine guidance without scaremongering. We're not trying to sell you anything. We're just trying to make sure you know what the risk of simply doing nothing is. Much has been made of the threat to vessels on the water from hackers. However, there is only limited available credible evidence to support claims of hacks at sea. Rather, the real threats on the water come from a lack of crew training and awareness and a culture which turns a blind eye to crew using their own devices at work (Bring Your Own Device, or BYOD) and plugging them into ship systems to charge them, thereby possibly releasing a malware they may have been inadvertently carrying onto the vessel.

Maritime cyber security survey results

In 2017, I.H.S. Fairplay conducted a maritime cyber security survey, to which 284 people responded. 34 percent of them said that their company had experienced a cyber-attack in the previous 12 months. Of those attacks, the majority were ransomware and phishing incidents; exactly the same sort of incidents affecting companies everywhere, and not at all specific to the maritime world.

The good news is that only 30 percent of those responding to the survey had no appointed information security manager or department, meaning that the majority of companies have a resource able to respond and mitigate any attack.   However, the survey did reveal that there are still a lot of employees who have not received cyber awareness training of any kind, which means the shipping industry must try harder, for its own security.

Additionally, only 66 percent of those questioned said that their company had an IT security policy, which is a serious cause for concern; IT security cannot be approached on an ad hoc, incident by incident basis. It's the security equivalent of plugging holes in a hull with cardboard. To underline that, 47 percent of those questioned believed that their organization's biggest cyber vulnerability was the staff. Hardly a glowing endorsement but, if you don't train your staff to be aware of threats, it's not surprising.

Mitigating the risk – train your staff

Imagine you're in charge of a company. You trust your staff to do everything. Except, it seems, ensure your bank accounts aren't handed over to cyber criminals or that your network is exposed to ransomware or malicious attack. It would seem to be a rather curious way to run a company.

The key to mitigating cyber-crime is training. Yes, you can put posters up; send company memoranda out; promote industry guidelines. But how many of your staff take those in? A robust workplace IT security policy is the first step, but that can only work when also supported by a training course where employees can see the risks through demonstrations, simulations and good teaching.

There are very simple changes that any company can make to ensure better security in the workplace. From enforcing a zero tolerance on BYOD, which is often disliked by the crew, to separating crew and administrative or operational networks, blanking unused USB ports and requiring monitors be turned away from public view to prevent "shoulder surfing" and a rule that all computers go into secure sleep mode when left unattended. For staff dealing with accounts, additional rules may be required to ensure the risks of phishing and social engineering (whale attack) are reduced.

You don't think your company is at risk? In November 2016, Europe's largest manufacturer of wires and electrical cables, Leoni AG, lost £34 million in a whale attack, when cyber criminals tricked finance staff into transferring money to the wrong bank account. £34 million. Lost… That should be read out to every board of directors.   And similar attacks take place every week.

In the last six months [fall 2017 to spring 2018], the shipping industry has seen several incidents in the sector, ranging from a data breach at Clarksons through to the damage done to Maersk by the WannaCry NotPetya variant sabotage/ransomware incident, which the company believes cost it as much as $300 million.

These are some of the reasons for the creation of the Maritime Cyber Alliance, a project created by CSO Alliance in partnership with Airbus Defence & Space. The aim is simple: connect maritime and oil and gas chief information security officers via a secure, private platform, allow verified cyber intrusions to be reported anonymously and provide members with threat alerts and tools to analyze malware and prevent attacks as well as offering workshops to promote best practice in the industry and listen to concerns.

February saw the Alliance participate in four workshops across the U.K., in Aberdeen for the offshore industry; Edinburgh for the ports community and Glasgow for ship management. Guest speakers included Kewal Rai, Policy Adviser for Cyber Security with the Department of Transport, Sergeant David Sanderson from Hampshire Police, Vic Start, Thomas de Menthiere and Jean Baptsiste Lopez of Airbus, among others.

Among the concerns raised by attendees were questions on mitigation of attacks, the impact of E.U.'s General Data Protection Regulation (GDPR) on the U.K. and how Airbus was delivering its solutions to users of the site. The Alliance is already gathering detailed cyber-crime incident reports from industry. We've seen examples; shipowners who lost two days' hire due to malware contamination via a USB stick, invoice fraud in the port, superyacht and ship broker sectors. The latter saw a ship broker's systems compromised by criminals who altered payment details to steal £500,000.

Luckily, in that case, the company's quick reaction, a court order and a rapid forensic investigation ensured they recovered the missing funds. We are starting to see multiple attempts of invoice fraud using privileged information, which means a vendor's company accounts have been compromised. The timely sharing and analysis of information will grow with the increased cyber-crime report data flow via the Cyber Alliance's crime reporting servers, based in Iceland in order to ensure anonymity. The solution, of course, is to ensure your company requires multiple sign-offs for any payments over a certain amount and pick up the phone to verify and vendor bank account changes. The risk of getting it wrong could bankrupt you. There's clearly a need for industry to take the lead on protection and, hopefully, the Maritime Cyber Alliance will enable that. Further workshops, which are all free to attend, are planned for the coming months.

Regulatory compliance

The next major hurdle facing companies around the globe comes in the shape of the GDPR, which comes in to force in May 2018. It will affect companies in every sector, but the maritime industry in particular, given its global reach.

In essence, the GDPR is the first data protection measure to affect the entire world. If your company holds or processes the personal data of E.U. citizens, people working for E.U. entities or trading with the E.U., then you're affected and will need to ensure that you're compliant with the new regulations. Failure to do so will result in huge fines. GDPR's definition of "personal data" is far broader than previous regulations, meaning that any information which can be used to identify an individual fall under it.

The new regulation introduces Privacy Impact Assessments (PIAs), which means that companies will be required to conducts PIAs wherever privacy breach risks are high in order to minimize risk to data subjects. Many companies may have to hire data protection officers in order to ensure compliance, while those companies dealing with EU crews will also want to take note of their liabilities in this regard.

The good news is that GDPR will also bring in common data breach protection notification requirements, so companies will be forced to report any breach of their systems within 72 hours, thus ensuring industry awareness and a better response time to potential vulnerabilities. This, in itself, may require staff training and is yet another aspect of GDPR companies need to be aware of.

For companies doing business in the E.U., which covers a vast swathe of the maritime industry, the NIS Directive covering network and information security also comes in to force in May 2018. In the U.K., the government has announced that organizations working in critical services like energy, transport, water and health can be fined up to £17 million as a "last resort" if they fail to demonstrate that their cyber security systems are equipped against attacks.

The NIS Directive requires organizations to have the right staff in place and the proper software to mitigate cyber-attack and intrusion. Private and public companies in each sector will be evaluated by regulators who will vet everything from infrastructure and issue fines for firms who fail.

"*Network and information systems give critical support to everyday activities, so it is absolutely vital that they are as secure as possible*," said Ciaran Martin, U.K. National Cyber Security Centre CEO, in a statement.

Ultimately, the new regulations will be of benefit to everyone, but ensuring your company meets the right standards will be crucial. The days where maritime cyber security amounted to just making sure you turned the office PC off are long gone. Today, cyber security demands board room level attention as well as vigilance from all employees, be they in head office or out on the water.

Cybersecurity in Maritime, Shivam Sargam, The Maritime Express, December 4, 2018

The cyber security in maritime is a matter to be mulled upon. The experts suggest the risk from a hostile attack on ship's system which allows the vessel to be operated remotely by the pirates and misguiding it to a port of their own choice. It may cause a catastrophic navigation error, a phishing attack or ransomware on the Master's PC. As of 2018, the global implementation of robust maritime cyber security policy is essentially non-existent.

IMO recommendations

IMO recommends the enforcement of cyber security in maritime. The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from present and future cyber threats and vulnerabilities. The recommendations on cyber security can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

The maritime cyber risk hints to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

Maritime Cyber security survey results

Near about 70% of senior maritime sector administrators in the US believe, the sector is prepared to respond to cyber-attacks, whereas half of that number believes their own businesses are ready. Out of 126 senior maritime administrators polled in a survey by US-based law firm Jones Walker, only 36% said their business is prepared to face the attacks of cyber.

According to the survey, the small and medium-sized companies are farther less prepared when compared to larger companies to counteract to the cyber security breach. The small-sized companies lack even in the most fundamental protections, exposing them to huge potential losses. 92% of small companies and 69% of medium-sized companies confirmed that they have no cyber insurance. The larger companies reported having cyber insurance. Almost 80% of large US maritime sector companies (with more than 400 employees) reported encountering a cyber-attack within the past years.

When asked regarding the companies' greatest cyber security exposure, the various respondents from large companies focused on external threats. The Medium and small companies offered a more mixed assessment of current threats. A worrying level of complacency among maritime industry is spread when talking of cyber security.

The consequences of financial aspects can be crippling. The companies that had been breached off in cyber security are more prepared now on. However, 36% of small company cyber-attack victims are still unsure about the reasons behind their breaches. On the whole, only 10% of the survey respondents reported against the cyber-attack over the past 12 months. While 12% reported that they have been successful in managing to tend off the pirates during the same time frame.

Nearly 80% of large US maritime industry companies (with more than 400 employees) reported facing a cyber-attack within the past year.

Years back, the attacks like piracy were a common threat and so physical defences are well understood. In contrast to that, the modern cyber and cyber-physical attacks aimed at ships are significantly less understood. Therefore, less preventable with current codes and practices.
The stealth ability and long attack duration's relating to cyber-attacks increase the number of cyber threats in general. The breach in maritime cyber security leaves an impact on business disruption, theft of information, finance, and cargo. It also damages the reputation, goods, and environment.

The maritime sector is a major role-player of global trade infrastructure and transportation. Furthermore, the significant amount of shipping-based travel crossing national lines creates an interesting geopolitical dimension to maritime cyber security, due to separate nations and their policies. Such policies are influenced by a nation's economic and environmental factors. Shipping being a different mode of transportation poses a unique cyber security problem. Ships have an entirely different system, different trip durations (months Vs hours), cargo volume etc. From passenger ships to large container vessels sailing on international waves, the vast majority vessels share two fundamental functions: navigation and propulsion. Both of which are supported by a plethora of hardware and increasingly advanced software controls. The standard navigation systems like Global Positioning Systems (GPS), Automatic Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS) have increased physical safety through international regulation. However, with their technological advances comes a new threat to the cyber security attack to exploit ships and the sailors. Once the spoofing (providing wrong data) or the jamming of the transmission is done the vessels are directed to false destinations. The alteration in the routes of the ship is done the attackers, to smuggle the drugs and other illegal goods. The criminal smuggling activities in the past few months are on a high list.

Recognizing the threats

However, there is the only limited availability of credible evidence to support claims of hacks at sea. The real threats at the sea come from a lack of crew training. The crew members' awareness of using their own devices at work (Bring Your Own Device, or BYOD) is essential. As plugging those into ship systems to charge them may possibly result in a malware. It might have been inadvertently carrying onto the vessel.

Mitigating the risk – train your staff
Ensuring the bank accounts to avoid the cyber-attacks or exposure of network is a big threat. The way to mitigate cyber-attacks is training. The minor changes like enforcing a zero tolerance on BYOD may be a help to keep the cyber security intact.

To separate crew and administrative or operational networks, blanking the unused USB ports and keeping the monitors turned away to prevent the "shoulder surfing" and a rule to keep the computers at into secure sleep mode when left unattended. The staff dealing with the accounts and additional rules may be required to ensure the vulnerabilities of phishing and social engineering (whale attack) may be lessened.

In November 2016, Europe's largest manufacturer or wires and electrical cables, Leoni AG, lost £34 million in a whale attack, when cyber criminals tricked finance staff into transferring money to the wrong bank account.

Similar attacks take place every week. In the last six months, the shipping industry has seen several incidents in the sector, ranging from a data breach at Clarksons through to the damage done to Maersk by the WannaCry NotPetya variant sabotage/ransomware incident, which the company believes cost it as much as $300 million.

Conclusion
The maritime is clearly trailing other sectors in critical national infrastructure and needs new approaches for the regulations. Several short terms training and new systems in long-term would be required.

The Unique factors in the shipping industry, particularly dynamic changes in maritime technology, and economy, social, and environmental elements, present significant cyber security challenges to protect this critical and most significant international infrastructure.
The guidelines and a mandatory policy from IMO can have significant, positive impact in real-world situations in combating both known as well as unknown cyber threats and thus that is the only rising hope for the cyber security in the maritime.

Maritime Cybersecurity using ISPS and ISM Codes, Alejandro Gomez Bermejo, He-Alert.org, Online Article viewed March 15, 2019

Introduction
Currently neither the IMO nor the national authorities have regulated on incorporating cybersecurity controls in the maritime sector. In this article I present some ideas to incorporate maritime cybersecurity policies, procedures and controls in vessel operations. First, I make a brief description of the IMO security ISPS and safety ISM codes. Then, I indicate how cybersecurity could be incorporated using these codes.

ISPS Code, Security of Ships and Port Facilities.

The guidelines for preventing deliberate attacks on ships and port facilities is defined in the International Ship and Port Facility Security Code ISPS adopted by the IMO International Maritime Organization in 2002.

The ISPS code applies to ships engaged on international voyages including passenger ships and cargo ships over 500 gross tonnage. The code does not does not apply to naval ships or Government ships used on non-commercial service. The ISPS code comprises a first part (A) of mandatory provisions and a second part (B) of optional provisions at the discretion of national authorities. The ISPS has been enforced in the European Union by EC regulation 725/2004 confirming as compulsory the provisions in part A and some of provisions in part B.

The Objectives of the ISPS Code are:

- Establish an international framework involving co-operation between Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade.
- Establish the respective roles and responsibilities of the Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security.
- Ensure the early and efficient collection and exchange of security-related information.
- Provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels.
- Ensure confidence that adequate and proportionate maritime security measures are in place.
- The threats considered in the ISPS Code are mainly of physical type. Ships are required to apply incremental protective security measures according to the following levels:
- Security level 1: level for which minimum appropriate protective security measures shall be maintained at all times.
- Security level 2: level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- Security level 3: level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.
- The ISPS contracting national governments are responsible for the following:
- Setting of the applicable security level.
- Approving a Port Facility Security Assessment and subsequent amendments to an approved assessment.
- Determining the port facilities which will be required to designate a Port Facility Security Officer.
- Approving a Port Facility Security Plan and subsequent amendments to an approved plan.
- Exercising control and compliance measures.
- Establishing the requirements for a Declaration of Security.

Ship Security Plans in ISPS

According to the ISPS code a ship security plan SSP needs to be created. The organization and procedures of the ship security plans SSP should establish:

- The duties and responsibilities of all shipboard personnel with a security role. The procedures or safeguards necessary to allow such continuous communications to be maintained at all times. The procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction.
- The procedures and practices to protect security sensitive information held in paper or electronic format.
- The type and maintenance requirements, of security and surveillance equipment and systems, if any.
- The procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns. The procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

The SSP is clearly focused on physical security. For example, its contents will include references to people responsibilities on the ship and on land, physical access controls to the ship, guards and patrols, CCTV surveillance and prevention and action against possible pirate attacks.
An example of the recommended content for the SSP (USCG) is shown below:

- Security organization of the vessel
- Personnel training
- Drills and exercises
- Records and documentation
- Response to change in MARSEC Level
- Procedures for interfacing with facilities and other vessels
- Declarations of Security (DoS)
- Communications
- Security systems and equipment maintenance
- Security measures for access control, including designated passenger access areas and employee access areas
- Security measures for restricted areas
- Security measures for handling cargo
- Security measures for delivery of vessel stores and bunkers
- Security measures for monitoring
- Security incident procedures
- Audits and Vessel Security Plan (VSP) amendments
- Vessel Security Assessment (VSA) report.

ISM Code. Safe Operation of Ships.
The guidelines for the safe operation of ships are defined in the IMO International Safety Management ISM code. This code was originally approved by IMO in 1993 and was made mandatory from 1998. The ISM Code applies to passenger ships irrespective of their tonnage and cargo ships over 500 gross tonnage. It does not apply to vessels of non-commercial use.

The objectives of the ISM Code are to ensure safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment, in particular to the marine environment and to property.   According to the ISM code, the safety management objectives of the shipping company should:

- Provide for safe practices in ship operation and a safe working environment.
- Assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards.
- Continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection.

Every shipping company should develop, implement and maintain a safety management system SMS which includes the following functional requirements:

- A safety and environmental-protection policy.
- Instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag State legislation.
- Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel;
- Procedures for reporting accidents and non-conformities with the provisions of this Code;
- Procedures to prepare for and respond to emergency situations.
- Procedures for internal audits and management reviews.

Safety Management Manual in ISM

The operation of the safety management system SMS must be documented and each ship should carry on board all documentation relevant to that ship. The documents used to describe and implement the safety management system may be referred to as the Safety Management Manual SMM. The SMM manual is focused on the safety of operations, people and the environment. An example of the recommended content for the SMM manual (USCG Vessel safety program) is shown below:

- Introduction
- Safety and Environmental Protection Policy
- Company Responsibility and Authority
- Designated Persons
- Master’s Responsibility
- Resources and Personnel
- Vessel Operating Procedures
- Emergency Preparedness
- Reporting Procedures
- Maintenance
- Documentation
- Company Verification and Review

Maritime Cybersecurity on Ships

Some safety management manuals SMM include references to information systems security on board. However, these references to information security or computer security are usually very basic. For example, the SMM will refer to the security measures of onboard computer systems such as protection with passwords, performing backups and protection of the equipment containing the SMM manual. The SSP manual will normally have a strong focus on physical security. SMM and SSP manuals will rarely include cybersecurity policies, controls or procedures. In my opinion, the Ship Security Plan SSP and Safety Management Manual SMM may be the appropriate documents to include references to maritime cybersecurity policies and controls such as:

- Risk analysis of information technology IT systems
- Preventive security measures deployed in the ship and ashore to mitigate risks in IT systems to an acceptable level.
- Internet access security policy indicating restrictions applicable depending on the operations being performed on the ship.
- Policy for the use of removable storage media such as USB sticks, external drives, CDs and DVDs.
- Policy and network access controls for the crew and wireless WiFi networks.
- Policy and procedures for updating and maintaining information and navigation systems.
- Physical and logical access controls to the various ship systems based on its sensitivity level.
- Authorization criteria for remote connections from the company office for system monitoring and maintenance.
- Contingency plan for information technology IT systems.
- Cyber-incident management procedures: detection, reporting, assessment and decision, response, recovery and lessons learned.
- Training and awareness of master, officers, engineers and crew on cybersecurity risks and controls. For example, a maritime cybersecurity policy should require disabling or limiting access to Internet and WiFi connections during sensitive operations such as port approaches, piloting and berthing operations.

Cybersecurity Manual and Procedures

Cybersecurity manuals, procedures and checklists should have their own identity and the supporting documentation should be incorporated in a Ship Cybersecurity Manual (MCSEC). The MCSEC could be referred from the SSP and SMM as in the following examples:

- The existence of a contingency plan for the ECDIS navigation systems should be in the SMM. In case there is a contingency, the details of the IT Systems Contingency Plan, including ECDIS, should be found in the MCSEC.
- Physical access control to different areas of the ship should be indicated in the SSP. Logical access controls for IT systems in the different physical areas should be found in the MCSEC.
- Ship position readings in ECDIS do not correspond with previous ECDIS readings or current visual fixes suggesting a system malfunction or deliberate interception. Besides following SMM recommended procedures for the safe navigation of the ship, the MCSEC cyber-incident management procedure should be consulted to assess the potential cyber-incident and respond appropriately.

It is very important to realize that the definition and documentation of the MCSEC manual and policies is only a first step. It is also necessary to deploy the cybersecurity procedures, controls and checklists, provide training, test regularly and verify the results in order to improve.

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.