An Integrated Maritime Cyber Security Policy Proposal

Conference Paper · August 2019

CITATIONS
0

READS
18

3 authors, including:

Alexandros Voliotis
University of Thessaly
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Ioannis Filippopoulos
Hellenic American University
13 PUBLICATIONS **5** CITATIONS
SEE PROFILE

An Integrated Maritime Cyber Security Policy Proposal

[1]STERGIOS OIKONOMOU [2]IOANNIS FILIPPOPOULOS [3]ALEXANDROS VOLIOTIS

[1,3]Dept. of Biochemistry and Biotechnology, University of Thessaly, Volos, Greece,
[2]Department of Computer Science, University of Thessaly, Lamia, Greece & Department of Informatics and Engineering, Hellenic American University, 436 Amherst Street, Nashua, New Hampshire 03063, USA
Email: [1]stergios.oikonomou@gmail.com, [2]yf@outlook.com.gr, [3]abwasp2000@yahoo.gr

***Abstract*—** The security environment of the twenty-first century has changed. There is no 100% security. The maritime industry as a part of the cyber domain is a very competitive and complex industry. Increasingly dependent on complex critical communication and information systems make this industry one of the most susceptible to cybersecurity attacks. Cyber threats and cyber-attacks are becoming more frequent and more sophisticated every day. As these attacks have been happening more frequency with serious consequences, cybersecurity has become a primary focus for the maritime industry. The cyber threats cannot be eliminated completely, but the risk can be greatly reduced to a level that allows maritime community to continue to prosper, and benefit from the huge opportunities that digital technology brings. Therefore, appropriate Cyber Defense measures and capabilities have to be in place to face and counter the threats from cyberspace. This will require having effective tools, a well-trained workforce and proper processes in place to detect, analyze, counter, and mitigate cyber threats and vulnerabilities.
To help understand the risks, this paper attempts to analyze the common cyber threats, the possible actors behind a cyber-attack as well as its anatomy. Furthermore, there is a report about the vulnerabilities in ship systems but the main purpose of this paper is to propose a cyber-security policy and its components for the maritime sector.

Keywords: *Maritime*, Cyber Defense Policy, Cyber Attacks, Vessels, Information Security, Cyber Security Policy, Cyber Attack, Integrity, Confidentiality, Availability.

I. CYBER SECURITY

A. What is cyber security?

One of the most appropriate short definition as given by Techtarget.com is: «Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access».
In an organization, people, processes, and technology must all complement one another to create an effective defense from cyber-attacks. People can be the weakest link or the strongest defence in an organization. As more than 80% of all reported information security and cyber incidents at sea are related to human error, the human element is one of the biggest vulnerabilities of the industry and must be a core part of the solution. Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information and last IT systems can be deployed to prevent or reduce the impact of cyber risks.
Last but not least, cyber security is everybody's responsibility.

B. The Importance of Cyber Security in Maritime

The global shipping industry is undergoing a technological revolution. Crews becoming smaller, ships becoming larger, and a growing reliance on automation all significantly worsen the risks from hackers. Modern maritime ships are often monitored and controlled remotely from shore-based facilities thousands of miles away to ensure efficiency. There are many different classes of vessels which tend to have different computer systems built into them. Many of those systems are designed to last more than three decades. Placed in another context, many ships operate outdated and unsupported operating systems. All this creates a new platform for hackers to conduct targeted cyber-attacks. Why to hack shipping companies? What are the motivations? A few may be:

- stealing money;
- stealing information;
- causing disruption or loss.

About stealing money: An attacker could trick a company to transfer money directly to him using the method "man-in-the-middle" through which the attacker establishes communication with the victims who think that they exchange messages between them, when in fact the entire conversation is controlled by the attacker and direct the companies' monies directly to him. Another way is by using ransomware (described in more details at subparagraph III.B.2), where the victim's computer or database is encrypted by the attackers. The victim then has to pay a ransom in order to get the key to decrypt data. According to a report published by the United Nations Office on Drugs and Crime, the World Bank and Interpol, «pirates of Somalia managed to claim some 3-400 million USD in ransom from 2005 to 2012. Out of 179 hijacked vessels in this period, ransom was paid for 152 vessels».
Stealing information: In shipping there is a large number and many different types of information with a great deal of value.
For example an attacker can steal information about shipping containers and the type of their content and the route they will follow. Such information may be sold to a competitive company or for investment purposes.

If we speak about the motivation causing disruption or loss we refer to the target to make systems and resources unavailable. Such attacks may be: cyber-attacks on port systems that may cause ports' shutdown, violation or even deletion of data that are used in a cargo terminal and may lead to terminal suspension until all the data restored.

II. CYBER THREATS

A Cyber Threat is any unauthorized attempt to gain access in a computer network. Nowadays there are many different kinds of cyber threats and the most important of these are presented below. Common Cyber threads are Phishing and Spear Phishing, Malware, Denial of Service (Dos), Inside Thread, Advance Persistent Threat (APT), Password Attacks.

III. CYBER ATTACK

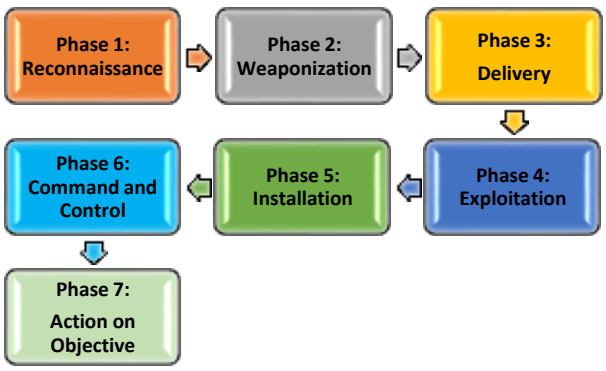
A. *Actors behind a cyber-attack*

There are various kinds of actors who are conducting cyber operations directly or indirectly against the maritime organizations, such operations can cause disruptive effect on the functioning of these organizations.

Picture 1: Cyber-attack actors

1) *Espionage*
2) *Hacktivism*
3) *Criminal*
4) *Terrorism*
5) *Business competitors*

B. *Anatomy of a cyber-attack*



Picture 2: Cyber-attack phases

1) *Phase 1: Reconnaissance*

Cyber attackers first identify the target, the vulnerabilities included, the best ways to exploit them in order to launch a cyber-attack. They only need a single point of entrance to get started, as anyone in an organization would suffice as a target.

2) *Phase 2: Weaponization*

The information that any cyber attacker gathers is used in order to change something that he discovered causing a favorable result for him.

3) *Phase 3: Delivery*

Following weaponization phase, it's time for the attackers to start their attack.

4) *Phase 4: Exploitation*

During the exploitation phase, the attacker takes advantage of discovered vulnerabilities.

5) *Phase 5: Installation*

Once the attacker gains access to the organization's network, he must ensure that he will continue to have that access as long he wishes.

6) *Phase 6: Command and control*

In this phase the attacker has unlimited access to the network. He can move deeper into the network. He can exfiltrate data, conduct DoS operations and anything malicious that he wants.

7) *Phase 7: Action on objective*

This is when the attacker comes to his real objectives and goes on to act on them. The objective could be anything such as stealing data, messing around with the operations of the company, cause mischief with the order-taking system and get things shipped to customers based on fake orders, shut down equipment, disable alarms etc.

C. *Vulnerabilities in Ship Systems*

Till recently, there was a belief that distance and isolation of vessels was a security barrier against cyber-attacks. However, this is wrong. Ships nowadays are using more and more onboard Information Technology (IT) and Operational Technology (OT) systems which are interconnected and connected to the internet. This interconnectivity increases the risk of exposure to internet-based and insider cyber-threats.

There should always be a distinction between IT and OT systems.

IT is an often-used and fitting term to describe business enterprise systems that move necessary data in order to support business-level operations including software, hardware and communication technologies.

OT is a domain complementary to IT that consists of hardware and software components and systems that directly monitors/controls physical devices and processes. Both IT and OT might be vulnerable to cyber threats.

At maritime industry there are a number of onboard systems which may be exposed to cyber risks. Vessels do not need to be attacked directly because an attack can happen via the company's shore-based IT systems and very easily penetrate the ship's critical OT systems. Maritime companies should make sure that they understand how shipboard systems might be connected to uncontrolled networks.

IV. CYBER POLICY

A. *Scope*

Cyber Security Policy serves a lot of purposes. The main purpose for a well-thought-out policy is to describe all the procedures to be followed in order to guard all the critical assets, equipment and data against cyber-attacks. Furthermore,

policy describes the user's roles, responsibilities and privileges. What is considered acceptable use? What are the security rules to be applied? The policy answers these questions and describes the user limitations. It contains procedures for responding to incidents that threaten the security of the company computer systems and network.
Ideally, a cyber security policy should be documented, reviewed, and maintained on a regular basis.

B. Cyber Security Policy Contents

1) Roles and Responsibilities

a) Security Operation Centre (SOC)

A Security Operation Centre (SOC) is a centralized facility with a dedicated security team inside, that has to exist in every maritime organization, in order to monitor, analyze and assess its network and IT-services against cyber threats. The required capabilities for SOC are: security monitoring, vulnerability analysis and pretesting, configuration test and security templates application, security inspection and risk analysis, malware, forensic analysis, audit and source code security support, conducting mitigation and counter-measures, incident management and coordination, systems and networks security assessment and Intruder detection. A SOC should be also able to organize Incident Handling Teams capable to react to incidents or attacks.

b) Company Cyber Security Officer (CCySO)

Every company should designate a Company Cyber Security Officer. A person designated as the CCySO may act as the supervisor of the Incident Handling Team.
The CCySO is shore-based personnel and should have knowledge, in some or all, of the following:

- Networks and operating system;
- System evaluations;
- System security penetration testing;
- Security operations/network monitoring;
- Security information and event management;
- Network mapping;
- Configuration of firewalls, routers and other security tools;
- Encryption systems;

The duties and responsibilities of the CCySO should also include, but not limited to:

- Analyze existing and future systems across the company, review security architectures, and develop solutions that integrate information security requirements to proactively protect information;
- Incident handling capability by monitoring, analyzing and responding to incidents;
- Conduct forensic analysis and review and assessment of security events and logs via sophisticated cyber security /event management tools;
- Conduct security risk assessments, and make recommendations of countermeasures to address risks, vulnerabilities and threats;
- Review and validate security documentation;
- Order the activation of the Contingency Plan and select the appropriate recovery strategy;
- Determine who should be notified if a cyber incident occurs.

c) Ship Cyber Security Officer (SCySO)

The SCySO is responsible for all security aspects of cyber-enabled systems on the ship, i.e. both the IT, OT and communications systems.
The SCySO should have knowledge of, in some or all of the following:

- How to inspect ship security measures;
- Emergency procedures contingency plan and other security plans;
- Proper management of security and communication sensitive information;
- Current cyber security threats;
- Recognition and detection of dangerous devices;
- Different types of techniques that are likely to be used to bypass security measures;
- The layout of the ship installed equipment;
- Monitor reports on incidents;
- Secure communications;
- How to recognize persons who are likely to threaten security.

The SCySO should also be responsible for:

- Ensuring that security measures are implemented, maintained and that all security incidents reported to the CCySO;
- Implementing and supporting network defense, access control, data protection and data transfer mechanisms;
- Taking backups from the system and implementation of the recovery plan;
- Training shipboard personnel and increase security awareness;
- Ensuring that ship security equipment is properly operated, tested, calibrated and maintained.

d) Ship Security Officer (SSO)

The SSO (master and ship duty officers with specific security duties) is responsible to ensure ship security. The SSO should have knowledge of:

- Facility security measures and operations from ships and ports;
- Undertaking regular security inspections of the ship;
- Backup plans in cooperation with SCySO;
- Ways to control and manage the crew ;
- Techniques used to circumvent security measures;

The SSO should also be responsible for:

- Reporting all security incidents to the SCySO;
- Ensuring that all shipboard personnel has the required security training and awareness;
- Conducting security inspections with SCySO at regular intervals;

e) Shipboard Personnel

Shipboard personnel should have sufficient knowledge and ability to:

- Recognizes characteristics and behavioral patterns of persons who are likely to threaten security;
- Uses communications with safety;
- Applies emergency procedures and contingency plans;
- Search (physical) persons, baggage, cargo, and ship's stores.

Finally, it should be noted that all crew members regardless of position and responsibility should be constantly vigilant.

2) Procedures

a) Physical Security and Access Control

Every ship should have specific security areas and security measures to control access. Efforts to control electronic and physical access of information systems are essential to ensure that sensitive data is retrieved or altered for legitimate and approved purposes only, otherwise the malicious actors could steal or alter important information, take control of the ship or damage critical systems.
Physical access of spaces containing IT/OT assets must be controlled by physical barriers and devices (doors, locks) with security cameras (CCTV) and only accessed by authorized personnel.
Access Control Lists (ACLs) for physical possession or contact with system assets (devices, systems, workstations, servers, network connections, etc.) must be kept up to date.
Each employee must have a unique user credential. Disable automatic saving passwords for all applications. Define clearly all the equipment which requires remote access and disable remote management for simple users.

b) Identification and Authentication

USER LOGON IDS

Every user shall have unique logon id and password. An access control system should identify each user and prevent unauthorized users from entering or using information resources. Users shall be responsible for the proper use or misuse of their logon ID.
All user login IDs must be audited at least twice yearly and should be removed when they are no longer in use. Logon IDs should also not be passed on from one user to another.
Users who desire to obtain access to workstations or networks must have a completed and signed a Network Access Form. This form must be signed by the SCySO or department head of each user requesting access.

PASSWORDS

Passwords are required to gain access to networks and workstations. Every user should select a unique password to obtain access to any electronic information both at the server and/or the workstation level. Passwords must be locked after a maximum of three (3) unsuccessful logon attempts and SCySO should be the only responsible person to reset passwords. When passwords are reset, the system must automatically ask for it to be changed.
All passwords must comply with the following restrictions in be difficult to guess and intercept them:

- Must be at least eight characters long;
- Must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
- Must be changed every 90 days. Compromised passwords shall be changed immediately.
- The previous five passwords cannot be reused.
- Shall not be shared, or written down on paper, or stored within a file or database on a workstation, and must be kept confidential.

CONFIDENTIALITY AGREEMENT

Users of information resources shall sign, as a prerequisite for employment, an appropriate confidentiality agreement via which they will declare that they «understand that any unauthorized use or disclosure of information residing on the information resource systems may result in disciplinary action, consistent to the policies and procedures of federal, state, and local agencies».
All the temporary staff and third-party staff not already covered by a confidentiality agreement shall sign such a document before accessing into information resource systems.

c) Network Security

Network security is crucial for a ship. There must be measures to secure the networks of a ship like the following:

- Unused ports from all network devices should be closed;
- Servers and other equipment containing sensitive data must be maintained in a secure location;
- Several types of perimeter security appliances like firewalls, IDS/IPS systems, must be used with secure configurations on them and changing all the default passwords;
- Access to network areas can be restricted by isolating them or by implementing firewalls, smart switches and routers;

d) Satellite and Radio Communication Systems

The most secure network is self-contained, with no access to the outside world, but this is not possible for most maritime transportation organizations. Communications with multiple organizations including port administrations, ships, marine facilities, trucking companies as well as within organizations is necessary. The satellite link provider is responsible for providing a secure satellite connection and, in cooperation with the shipping company, will have to decide on the measures taken to ensure that it is safe. It must prevent illegitimate connections gaining access to the onboard systems. It must use interfaces with security control software provided from the communication equipment. If using a VPN, the data traffic should be encrypted. Ensure that available Wi-Fi signals do not permit access to sensitive data or functions. At last, in front of the servers and computers connected to the network there should be deployed a firewall.

e) Printers and External Devices

Transferring data from uncontrolled to controlled systems is a major risk. Nowadays the use of removable media with malicious content, is perhaps the main way to gain illegal access to networks and devices. Companies must ensure that external devices are not used to transfer information between uncontrolled and controlled systems. The best is to prevent all employees to use their own devices. If so authorized, the external devices should be password-protected and encrypted. All external devices must to be scanned in a computer that is not connected to the ship's controlled networks. SCySO should perform periodic scans of the system and should do real-time scans of files derived from external sources as files are downloaded, opened, or executed. If it is not possible to scan the removable media on board, then the scan could be done prior to boarding.

f) Social Media and Internet Usage

Nowadays the use of social media is very popular and becoming an integral part of business. Companies use social media as means to advertise and keep in touch with clients. Personal use of social media in the workplace must permitted, subject to certain conditions, as follows:

- It must not be overused but must be minimal and take place substantially outside of normal working hours and the company should withdraw the use permission at any time;

- Do not post material in breach of companies copyrights;
- Employees must never disclose commercially sensitive or confidential information because social media activity of the employees in the target company will be monitored to extract information about the systems and any technology vulnerabilities assessed;
- Employees should avoid social media communications that might be misconstrued in a way that could damage the business reputation, even indirectly;
- Employees online profiles must not contain the company name;
- If employees see social media content that disparages or reflects poorly on company, they should contact SCySO immediately;
- Be aware though that even if you make it clear that your views on some topics do not represent those of the organization, comments could still damage the company's reputation;
- All users personally are responsible for what they communicate on social media sites outside the workplace, for example at home, using their own equipment. Users must always be mindful of contributions and what disclose about the company;

Limited personal use of the internet or email at work is acceptable if it doesn't interfere with users' normal duties. Such use should take place substantially outside of normal working hours, for example, breaks, lunchtime. Users can access non-business related sites, but are personally responsible for what they view. They must not use company's equipment to access the internet either from within or from outside the company network and they may not upload, download, use, any images, text, or software which:

- Are not permitted from the SCySO through the «whitelist»;
- Make employees not to work productively (like games);
- Encourage or promote activities which would, if conducted, be illegal or unlawful;
- Involve activities outside the scope of user's responsibilities - for example, unauthorized selling/advertising of goods and services;
- Might affect or have the potential to affect the performance of, damage or overload the system, network and/or external communications in any way;
- Might be defamatory or adversely impact on the image of company.

Additionally, users must not include anything in an email which they cannot or are not prepared to account for. Care should be taken when adding attachments to emails. It is better not to use attachments, but if this is necessary, no attachment should exceed 20Mb in size. The auto-forwarding facility within the company's email system should not be used to forward work emails to private accounts (e.g. Gmail or Yahoo). Large files should be compressed. Users must not download through their email, any software, executable files or image files (GIFs and JPGs) unless they have obtained prior permission from SCySO.

g) Monitoring of Log Files and Alerts

If a maritime company wants to identify early and successfully address cyber-attacks, must have a good log files monitoring policy. Reviewing security reports, log files and alerts is a specialized ability which require a cyber security analyst in order to be most effective. Companies must create and implement a log retention policy that specifies how long log data should be maintained. This will be extremely helpful for the analysis, because older log entries may show reconnaissance activity or previous instances of similar attacks because incidents may not be discovered until days, weeks, or even months later. Every hardware system in the company's network generates some type of log file. All the systems using either Microsoft or Unix software produce logs. Event Log Management is a key component of compliance initiatives, since it can be monitored, audited, and reported on file access, unauthorized activity by users, and policy changes. The best options is to place an IDS or IPS sensor behind the firewall, to monitor and filter traffic between the internet and the internal network and alert SCySO for any cyber incident.

h) Antivirus Updates and Software Patches

Many maritime organizations don't apply patches often and timely, to fix vulnerabilities and protect their systems. Patching is one of the most important steps that a maritime organization can take to reduce exploitations from cyber threats in software and computer-based systems.

First, companies should only use authorized software on their systems. For this purpose, it's better for the company to have a list (whitelist) with all the software which is permitted to be used. Then, it is important for antivirus updates and software patches to be distributed to ships on a timely basis.

In each software, application or operating system, there are potential vulnerabilities which could be exploited by malicious cyber actors. Patching is the process of adding software code to eliminate a vulnerability and ensure the integrity of data residing on an IT/OT system. However, patch management can be a tough process. Vulnerabilities and fixes must be identified, analyzed, and tested before patches can be deployed and implemented. A tool that scans automatically all the systems for vulnerabilities is essential. Assigning a person to be responsible for the updates and reporting completion to the CCySO. Functional systems which are essential for the operation of the vessel may be updated on company's ashore facilities.

i) Intrusion Detection and Response

Having (and practicing) an incident response plan is probably one of the most crucial steps that any company must take. Every company should have systems like IDSs in place, to detect intrusions and respond to them. A clear and concise plan of action will help neutralize any intrusion into a network and mitigate potential damage. This plan should be tested continuously with exercises, examining its effectiveness in dealing with the cyber incidents. The incident response and the damages assessment should be also considered.

j) User Awareness and Training

Continuous training and awareness of both crew members and simple workers of a shipping company are essential elements to mitigate and effectively address cyber risks. Training should be tailored for all the staff, onboard and onshore, according to each one's duties. SCySO is responsible for training the shipboard personnel and increasing their security awareness and SSO must ensure that every one of them has the required security training and cyber awareness. Continuous exercises should be carried out to simulate possible incidents and their outcomes must to be considered for future exercises, but also to all participants, in order to see how their actions could affect the

ship or the entire company. Finally, all crew members in accordance to the cyber security policy should at least be aware of:

- How to use the secure personal and other external devices (removable media, etc.) before connecting them to vessel's systems;
- The risks related to emails and how to utilize email in a safe manner;
- How to use social media and internet with safety;
- How to install and maintain software on vessel hardware with safety;
- How to safeguard user information, passwords, etc.;
- Recognize cyber risks in relation to the physical presence of non-authorized personnel;
- How to detect suspicious activity and how to report a possible cyber incident;
- The consequences of cyber-attacks on the safety of the vessel;

k) Recovery

Taking steps to put backups in place, allows the organization to continue its operations despite a successful cyber-attack.

The frequency of backups depends on the frequency that new data was introduced and how critical these are. SCySO should take backups regularly, using different storage media and he is responsible to do periodic recovery tests from backup site. External media such as dedicated external drives, recordable CD or DVD, should be available to the crew for data backup. Ensure that hardware is up-to-date and capable of recovering data. Since the portable backup drive can potentially contain sensitive information it should be protected by encryption and kept in designated secure locked location. Recovery plan should be implemented from the SCySO.

Another good practice is to store backed-up data offsite. In this case, data is backed up at the company's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, the company contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility.

3) Cyber Security Risk Assessment

Risk assessment is the process which collects information and assigns values to risks for informing priorities, defining the needs for critical system protection, and developing courses of action. It doesn't provide permanent information and it needs to be updated on a regular basis.

Risk assessment includes the following:

- Mapping all the system assets (hardware, connections) that are at risk. This can be done for example with an automated discovery tool;
- Identification of the cyber threats in the systems. As mentioned above, these threats could be malware, phishing, spear phishing, social engineering, DoS, inside threats, APTs, or actors like espionages, hacktivists, criminals, terrorists, business competitors etc.;
- Identification of the vulnerabilities in the systems. Here are mentioned specific vulnerabilities that exist and could compromise the IT and OT equipment and ship network;
- Analyze the impacts of the vulnerabilities. The analysis of the impacts resulting from each vulnerability determines to which degree the security state of the system affects;
- Determination of the risks. Here assesses the level of risks to the system associated with vulnerabilities mentioned above;
- Documentation. Any findings should be documented for further and future use.

4) Cyber Security Contingency Plan

a) What is Cyber Contingency Plan?

A cyber security contingency plan helps a maritime company to respond effectively to cyber incidents. Contingency planning is a necessary component for the business continuity and disaster recovery. It should be based on a cyber security policy that describes the actions and the steps to be taken when a cyber incident has occurred or is likely to occur.

According to the NIST Special Publication 800-34, there are some steps for a cyber security contingency plan:

- Develop the cyber security contingency planning policy statement;
- Conduct the business impact analysis (BIA);
- Identify preventive controls;
- Develop recovery strategies;
- Develop a contingency plan;
- Testing, training and exercises;
- Plan maintenance.

b) Develop the Cyber Security Contingency Planning Policy Statement

Cyber Security Contingency Policy Statement should give all necessary elements to achieve the policy purpose and should assign specific responsibilities to specific staff. For a maritime organization, the contingency policy should be developed not only for the ships but also for offshore installations and should evaluate the IT/OT equipment and systems, mention the kinds of disasters, operations of the systems, staff training requirements and estimated time to restore the IT/OT systems. The basic elements of the policy should be known to all employees onboard and onshore, according to each one's duties. The responsible person to start the activation of the Contingency Plan is the CCySO.

c) Conduct the Business Impact Analysis (BIA)

BIA is the process by which a maritime organization collects information and identifies the critical components about its system, as well as the threats that the system may face, the risks that these threats can cause and how they can affect the organization. According to the NIST Special Publication 800-34 the BIA has the following phases:

- Identify Critical IT Resources.

In this phase, CCySO finds all the critical system components, identifies the required resources to operate them, and finds all the persons that use the system network in any way

- Identify Disruption Impacts and Allowable Outage Times

In this phase, CCySO analyzes the previous critical resources and determines the impacts on IT operations if a given resource is disrupted or damaged. Allowable outage times indicates the maximum time that an IT system can be unavailable before it causes a significant impact on the system.

- Develop Recovery Priorities

The impact and allowable outage times from the previous step enables the CCySO to develop recovery priorities that will be implemented during cyber contingency plan activation that will

allow the maritime organization to determine the order that systems should be restored or recovered.

d) Identify Preventive Controls

Armed with the results of the BIA, a maritime organization can begin to take preventive measures to reduce the effects of system disruptions, increase system availability and to reduce contingency life cycle costs. Some common measures are firewalls, UPS, antivirus software, frequent backups, offsite storage of backup media, least-privilege access controls etc.

e) Develop Recovery Strategies

Recovery strategies help the organization to recover from an incident. The strategies should always prioritize critical functions, address the impacts identified in the BIA, take into account factors like allowable outage time and security. Furthermore, these strategies should include a combination of methods as mentioned in subparagraph V.B.2.k.

f) Develop a Contingency Plan

The development of the contingency plan is the main phase in implementing a comprehensive contingency planning program. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements. Contains detailed roles, responsibilities, teams, and procedures and includes technical information designed to support contingency operations that are tailored to the organization, information system, and its requirements. There are three phases that govern actions to be taken following a system disruption:

- Activation/Notification Phase describes the process of activating the plan based on outage impacts and notifying recovery personnel
- Recovery Phase details a suggested course of action for responsible staff to restore system operations at an alternate site or using contingency capabilities
- Reconstitution Phase includes activities to test and validate system capability and functionality and outlines actions that can be taken to return the system to normal operating condition and prepare the system against future outages

g) Testing, Training and Exercises

Contingency plan can be very complex. Testing this plan is necessary if the maritime organization wants to be sure that it is effective. Organizations need to take many decisions such as who does what and where, and what to do if it doesn't work. No one never wants to find out that the plan was poor during a crisis. Each contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The company should conduct training classes and exercises to ensure that the plan is effective. Test results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Important players should understand what their role is. Simulating a cyber disaster or performing testing to validate plan's effectiveness is necessary. Anything anyone can learn in a non-stress situation will be invaluable when the real thing happens.

h) Plan Maintenance

Nothing is ever static when dealing with cyber security. The plan should be a living document. Companies will need to re-evaluate their cyber contingency plans on a regular (preferably scheduled) basis, especially if there are relevant technological, operational, and personnel changes, to ensure that it is consistent with the risks the organization is facing. Every modification of the plan should be coordinated through the CCySO and should be recorded. The contingency plan contains sensitive operational and personnel information, therefore its distribution should be marked accordingly and controlled.

5) Cyber Incident Handling Process in the Maritime

Cyber defence requires mechanisms and procedures on the base of ongoing preparation in order to prevent, detect, respond, mitigate and recover from attacks affecting the confidentiality, integrity and availability of information and of supporting system services and resources. Having an established and rehearsed plan of action which a maritime organization executes after identifying a cybersecurity attack is crucial to limiting the damages. An effective plan should be comprehensive, covering every aspect of the incident. Mechanisms may be seen in a circle with four phases, as below:

- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post-Incident Activity

a) Preparation

The main aim of this phase is to prevent incidents by building up resilience and by using security controls measures. A good preparation is the key to success. Not preparing for a cyber-incident increases the risks impacting maritime operations. First step to be prepared for a cyber incident is to do an impact assessment.

The next step is to determine the kind of equipment and the cost of it in order to protect the assets that are critical to port and maritime operations. Maritime organizations must keep in mind that it may not make sense to spend a lot of money protecting a device unless the value of the information and data it stores or processes is operationally critical. The cost of protecting the file server for example is not just the cost of replacement or repair or the cost of backup, but also the cost to the organization if the information and data that stored on it will lost.

Another important part of this phase is to train the personnel to raise their cyber awareness. Every person in a maritime organization must have a basic training in cyber awareness focusing on impacts of cyber incidents and cyber-attacks. This is the best protection. In addition, ensure that users are made aware of the lessons learned following a cyber incident. A small investment in user training can turn into significant savings for the organization when a threat is avoided by a trained user. Users should also know the responsible person to which they will report any suspicious activity. Maritime organizations must create an incident handling team led by CCySO to be prepared to respond if an event occurs. Companies should decide who is in charge if an event happens. Maritime organizations should also take part in risk assessment. Frequent risk assessments of systems and applications help to identify vital resources and the way to prioritize them during a cyber incident.

b) Detection & Analysis

The most challenging and also the most important part is to detect and analyze possible incidents. Early detection of an incident allows the maritime organizations to respond before it escalates any further.

When an unusual action or network behavior is noticed, it should be reported immediately by the users. People have to be trained for being suspicious and for recognizing abnormal

behavior of their systems. This abnormal behavior may not only relate to incidents that have already occurred or are occurring at that time, but may also relate to incidents that indicate that they may happen in the future. All these different categories of incidents should be perceived and identified using many different sources, like IDS or IPS systems, log files, publicly available information, and people. Different types of security software systems should be used (not all systems detect all incidents), as well as third party monitoring.

When an incident occurs, the incident handling team should immediately start recording all facts regarding the incident. Then, the team should perform an initial analysis to determine for example which system or application is affected, who is responsible, what tools are being used etc. After this, the team must ensure a fast and coordinate reaction and report the incident to the public. In particular when more than one incident occurs, handling should not be handled on a first-come, first-served basis.

Ultimately, detecting and analyzing a cyber incident is the main key to quick return to normal operations with minimal disruption.

c) Containment Eradication & Recovery

When an incident occurs, it must be contained to gain valuable time for reaction and prevent further damage.

The key is to have a strategy already in place, based on known threats. This strategy should support rapid decision-making, also define acceptable risks in dealing with incidents, identify the different kinds of attacking hosts and consider the specifics and individual aspects of each incident type.

If an incident is only contained without eliminating the problems it has created, it will most likely continue to create more and more problems. This is the eradication phase, where all the "faults" created by the incident are detected and eliminated.

Then follows the recovery phase. At this phase, all necessary steps are taken in order to restore systems to its normal operations such as use of backups, patches installations etc. or in large-scale incidents maybe even rebuild the all system from beginning.

d) Post-Incident Activity

This phase aims to learning from incidents, reflecting and reviewing what happened, how the incident was managed and what can be improved.

The key to a proper lessons learned regime is holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after smaller incidents.

As incidents performed through new attack methods, they are of widespread concern and interest. Respective information on this as well as on the incident handling, should be shared as well as reported to other organizations. Prepared documentation should be updated as a result of the lessons learned meeting. Because of the changing nature of information technology and changes in personnel, the incident handling team should review all related documentation and procedures for handling incidents at designated intervals.

At the end, an important post-incident activity creates a follow-up report for each incident, which can be used as «best practice» for future incident handling and data collection on incident handling (resources, time, and number) in order to justify future organizational changes as well as funding issues.

V. CONCLUSIONS

Although at the past the cyber security was something that didn't concern the maritime industry, the last few years fortunately there has been a gradual change in the mindset of the industry, and cyber security is now perceived as genuine threat and is a necessary element for the safe and efficient operation of all maritime organizations. Cybersecurity risks continue to grow exponentially around the world and greatly influence the maritime which uses complex critical IT and OT systems which have several vulnerabilities and should be protected against cyber threats.

Taking into account the modern trends of shipping that lead it to fully autonomous vessels then it is understood that cyber security becomes even more important.

The aim of this paper is to analyze the common cyber threats, the possible actors behind a cyber-attack as well as its anatomy. Furthermore, give a short report about the vulnerabilities in ship systems but the main purpose is to give a cyber security policy and its components for the maritime sector.

The creation of a cyber security policy with: specific roles and responsibilities for the users, secure procedures, and the existence of plans to deal with the different cyber risks are essential elements in order to tackle and reduce the number of cyber-attacks more effectively in order to allow maritime community to continue to prosper.

REFERENCES

[1] Trend Micro (2014). A security evaluation of automatic identification systems, Available at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais

[2] Understanding Cyber risk: Best practices for Canada’s Maritime sector, Transport Canada.

[3] SANS Institute (2017), Reply to Request for Information (RFI), Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development.

[4] Safety4Sea (2018). The seven phases of a cyber attack. Available at https://safety4sea.com/the-seven-phases-of-a-cyber-attack

[5] Safety4Sea (2018). 10 steps to maritime cyber security. Available at https://safety4sea.com/10-steps-to-maritime-cyber-security

[6] Safety4Sea (2018). Understanding the cyber risk at sea. Available at https://safety4sea.com/understanding-the-cyber-risk-at-sea.

[7] The Maritime Executive (2018), The Seven Phases of a Cyber Attack, Available at: https://www.maritime-executive.com/blog/the-seven-phases-of-a-cyber-attack#gs.

[8] The Guidelines on Cyber Security Onboard Ships, version 3, Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL

[9] MTI Network, Maritime Cyber Security, January 2016, Available at: https://www.flipsnack.com/mtinetwork/mti-network-cyber-security-report-2016.html

[10] National Institute of Standards and Technology (NIST), Contingency Planning Guide for Information Technology Systems, Special Publication 800-34, (June 2002).

[11] National Institute of Standards and Technology (NIST), Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2, (August 20120.

[12] SOPHOS, Threatsaurus, The A-Z of computer and data security threats, (2013).

[13] SBIR-STTR, America’s seed fund, Introduction to cyberthreats, course10 - tutorial2, Available at https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf

[14] Rapid7, Common Types of Cybersecurity Attacks. Available at https://www.rapid7.com/fundamentals/types-of-attacks, (2018)

[15] Gnostech Inc (2018), Cyber Incident Response in the Maritime Enviroment, Available at https://www.gnostech.com/maritime-blog/cyber-incident-response-maritime-environment-part-1,2,3,4.

[16] HM Government, National Cyber Security Strategy 2016-2021, (2016).

[17] National Cyber Security Center, Cyber Attacks White Papers, Common Cyber attacks: Reducing the impact, (2016).

[18] Institution of Engineering and Technology (IET), Hugh Boyes and Roy Isbell, Code of Practice - Cyber security for Ships.

[19] UCSB Information Security (2015), Inventories. Available at https://security.ucsb.edu/faculty-staff/inventories.

[20] Central Intelligence Agency (CIA), Carrers & Internships, Available at https://www.cia.gov/careers/opportunities/support-professional/information-assurance.html#job-details-tab2

[21] Bunkerspot, Limassol based shipping company victim of cyber fraud, Available at https://www.bunkerspot.com/latest-news/40447-global-limassol-based-shipping-company-victim-of-cyber-fraud

[22] FutureDirections (21 August 2018), The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges, Available at http://www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/

[23] Dejan Kosutic, 9 Steps to Cybersecurity, (2012).

[24] Edith Cowan University, A critical analysis of security vulnerabilities and countermeasures in a smart ship system, Dennis Bothur, Guanglou Zheng, Craig Valli, (2017)

[25] Techopedia, definitions, Available at https://www.techopedia.com

[26] Agence Nationale De la Securite Des Systemes d'Information, Thierry COQUIL,Guillaume POUPARD, Best Practices For Cyber Security On-Board Ships, (2016)

[27] Blank Rome Maritime, Maritime Cybersecurity: A Growing Threat Goes Unanswered, Kate B. Belmont, (2015)

[28] National Cyber Security Center, The cyber threat to UK business, (2016/1017) report.

[29] JRCS Corporation, Engine Control Console, Available at https://www.jrcs.co.jp/en/products/detail/engine-control-console

[30] The North of England P&I Association, Cyber Risks in Shipping, (June 2016)

[31] Safety4Sea (2017). Inmarsat takes mature approach to maritime cyber security Available at https://safety4sea.com/inmarsat-takes-mature-approach-maritime-cyber-security/

[32] Maritime Security Review (14 June 2018), The maritime cyber threat, Why 50.000 ships are so vulnerable to cyberattacks, Available at http://www.marsecreview.com/2018/06/the-maritime-cyber-threat.

[33] CyberKeel, Copenhagen, Denmark, Maritime Cyber Risks,(pages:16-19), Available at www.cyberkeel.com, (2014)

[34] International Armour Co, Defence and Security, Maritime Cyber Security, Available at https://www.armour.gr/catalogues/pdf/CyberSecurityOnBoard.pdf

[35] National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1, (September 2012).

[36] Royal Belgian Institute of Marine Engineers, The ship's electrical network, engine control and automation, Kari Valkeejärvi, Marine Technology, Wärtsilä Corporation

[37] Marineinsight, What Are The Duties Of Ship Security Officer (SSO)? Available at https://www.marineinsight.com/marine-safety/what-are-the-duties-of-ship-security-officer-sso/

[38] Wikipedia, AIS, Available at https://en.wikipedia.org/wiki/Automatic_identification_system

[39] MarineInsight, What is Ship Security Alert System (SSAS)?, Available at https://www.marineinsight.com/marine-piracy-marine/what-is-ship-security-alert-system-ssas/, (2018)

[40] I Filippopoulos et all, (2018), Transferring Structured Data and applying business processes in remote Vessel's environments using the" InfoNet" Platform, 2018 IEEE South-Eastern European Design Automation, Computer Engineering, Computer Networks and Society Media Conference (SEEDA_CECNSM).

[41] Wikipedia, Dynamic Positioning, Available: https://en.wikipedia.org/wiki/Dynamic_positioning

[42] Wikipedia, Global Maritime Distress and Safety System, Available at https://en.wikipedia.org/wiki/Global_Maritime_Distress_and_Safety_System

[43] MarineInsight, Marine Radars and Their Use in the Shipping Industry, Available at https://www.marineinsight.com/marine-navigation/marine-radars-and-their-use-in-the-shipping-industry, (2017)

[44] Wikipedia, Voyage Data Recorder, Available at: https://en.wikipedia.org/wiki/Voyage_data_recorder

[45] Wikipedia, Bridge Navigational Watch Alarm System, Available at: https://en.wikipedia.org/wiki/Bridge_navigational_watch_alarm_system

[46] I Filippopoulos et all, (2017), Collecting and using vessel's live data from on board equipment using "Internet of Vessels (IoV) platform", 2017 IEEE South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM).

[47] Wikipedia, Advanced Persistent Threat, Available at https://en.wikipedia.org/wiki/Advanced_persistent_threat

[48] Gnostech Inc (2017), Maritime Cyber Vulnerabilities and Hacking in the News, Available at https://www.gnostech.com/maritime-blog/maritime-cyber-vulnerabilities-hackings-news/

[49] International Maritime Organization (IMO), Measures to Enhance Maritime Security, (17 May 2016)