Issues and concerns in the maritime education regarding cyber risk management

Dimitar Komitov[1, *]
Nikola Vaptsarov Naval Academy, Varna, Bulgaria[1]
d.komitov@nvna.eu

Abstract: *In accordance with Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems" the companies must implement the issues to their Safety Management Systems no later than the first annual verification of the company's Document of Compliance after 01 January 2021. Some of the biggest companies and associations from the industry have published their own Guidelines on Cyber Security Onboard Ships. However, the question on ship's cyber security is still not implemented in the syllabuses. As per International Ship and Port Facility Security Code (ISPS Code), part B, 8.3.5 the ship's security assessment should include radio and telecommunication systems, including computer systems and networks. This necessitates finding answers to the following questions: whether the Ship's Security Plan has to be revised to include the appropriate measures to protect both equipment and communication links or Cyber security plan itself will be enough to cover the issues; whether the Cyber Security Officer (CSO) will be the person who will tackle the problem or the companies have to hire a well-qualified additional person; whether such a person has to be a mariner or IT specialist. The aim of this article is research regarding implementation of Maritime Cyber Risk Management requirements to the vessel's Ship Security Plan (SSP) and qualification of the person responsible for companies' fleet cyber security.*
KEYWORDS*: SECURITY PLAN; CYBER, ISPS CODE, SSP*

1. Introduction

Maritime cybersecurity is a problem which despite getting more and more attention, is still a major reason for concerns. Many organizations are involved in the issue: IMO, INTERCARGO, INTERTANKO, IUMI…

In general, the cyber security policy of each Ship's management Company provides guidelines to ensure the following:

• Confidentiality: Any important information that should be kept confidential and to protect access to confidential data and safety critical systems by placing a robust password control policy.

• Integrity: Maintain the integrity of information assets to keep everything complete, intact, and uncorrupted.

• Availability: Maintain the availability of systems, services, and information as and when required.

Cyber security requires an interdisciplinary approach and a comprehensive governance commitment to ensure that all aspects of the business are aligned to support effective cyber security practices.

2. Principality's cyber security system's characteristics

A cyber security framework is a set of cyber security activities, desired outcomes and applicable references that are common across critical infrastructure sectors. These frameworks can present industry standards guidelines and practices in a manner that allows for communication of cyber security activities and outcomes across the group both onshore and onboard vessels. Any shipping company identifies the need to establish and maintain an appropriate governance and risk management framework to identify and address risks for communications, networks and services. The cyber security framework functions include the following:

• Identify which assets need securing, as well as the threats and risks to them.
• Protect assets with the appropriate safeguards.
• Detect intrusions, breaches and unauthorized access.
• Respond to a potential cyber security event.
• Recover from a cyber security event by restoring normal operations and services.

According to the professor and former director of Information Security Group Keith Martin [1] in the sea at the moment is around 50,000 ships which are highly vulnerable for cyber attacks. In 2015 cybersecurity experts presented how easy it is to hack vessels [2]. They found security holes in Global Positioning System (GPS), Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS) used for viewing digital nautical charts. Taking control over these devices might easily send the ship of the course while faking correct course on display. The International Maritime Organization (IMO), the United Nations (UN) body responsible for creating maritime regulations was really late in case of cybersecurity recommendation because just in 2014 consulted what maritime cybersecurity guidelines should contain. Two years after that, they published first guidelines on cybersecurity risk management, but it was too general therefore not helpful with fighting against the hacker.

There is various equipment on board that can be classified into two categories:

• Information Technology (IT) equipment
• Operational Technology (OT) equipment

The IT and OT equipment on board are further broadly categorized as:

• Access Control systems
• Bridge systems
• Cargo management systems
• Communication, PA systems
• Propulsion and power management systems
• Administrative and crew welfare systems

The critical OT equipment is defined as a system, failure of which can immediately impact the safe operation of the ship or can directly result in a commercial loss/exposure. For the purpose of cyber security, below mentioned equipment of the vessel is identified as the OT critical equipment:

• RADAR (both X-band and S-band)
• AIS
• ECDIS
• GPS
• VSAT
• FBB
• Digital publication computer (CHARTCO / ADP & eNP publication PC Main & BackUp)
• Loading program / Stress monitoring system / ODM (Oil Discharge Monitor)
• Main Engine Control and Safety System

IT systems manage data while OT systems control the physical world and differ from traditional IT systems. OT is hardware and software that directly monitors/controls physical devices and processes, whereas IT covers the spectrum of technologies for information processing, including software, hardware and communication technologies. Traditionally OT and IT have been separated, but with the prevalence of the internet, OT and IT are coming closer as historically stand-alone systems are becoming integrated. Consequently, disruption of the operation of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment and ship's operation. Typical differences between IT and OT systems can be seen in the table below:

Table 1: *Differences between IT and OT systems*

Category	IT System	OT System
System operation	*systems are designed for use with commonly	*differing and possibly proprietary operating

	known operating systems *upgrades are straightforward with the availability of automated deployment tools	systems often without built-in security capabilities *software changes must be carefully made according to maker's instructions because of the specialised control algorithms and possible involvement of modified hardware and software
Resource constraints	*systems are specified with enough resources to support the addition of third-party applications such as security solutions	*systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities
Performance requirements	*non real time *response must be consistent *less critical emergency interaction *tightly restricted access control can be implemented to the degree necessary for security	*real time *response is time critical *response to human and any other emergency interaction is critical *access to OT should be strictly controlled but should not hamper or interfere with human machine interaction
Availability (reliability) requirements	*responses such as rebooting are acceptable *availability deficiencies may be tolerated depending on the system's operational requirements	*responses such as rebooting may not be acceptable because of operational requirements *availability requirements may necessitate backup systems
risk management requirements	* manage data *data confidentiality and integrity is paramount *fault tolerance may be less important *risk impacts may cause delay of: ships clearance, commencement of loading/discharging, commercial and business operations	*control physical world *safety is paramount, followed by protection of the process *fault tolerance is essential even momentary downtime may not be acceptable *risk impacts our regulatory non-compliance, as well as harm to the personnel on board, the environment, equipment and/or cargo

3. Cyber security threat identification

In general, cyber-attacks can be categorized as "untargeted" and "targeted".

"Untargeted" are attacks where a company or a ship's systems and data are one of many potential targets and include the following tools and techniques:

- Malware – Malicious software designed to access or damage a computer without the knowledge of the owner. Such types include trojans, ransomware (i.e., data encryption on systems until a ransom is paid), spyware, viruses and worms. Malware software may also exploit known deficiencies and problems in outdated / unpatched business software. The term "exploit" usually refers to the use of a software or code, which is designed to take advantage of and manipulate a problem in another computer, software, or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction and/or error in protocol implementation and can be triggered remotely, or locally, often executed by the user, sometimes distributed via links in email attachments or though malicious websites.
- Phishing – Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.
- Water holing – Establishing a fake website or compromising a genuine website to exploit visitors.
- Scanning – Attacking large portions of the internet at random.

"Targeted" are attacks where a company or a ship's systems and data are the intended target and include the following tools and techniques:

- Social engineering – A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures normally, but not exclusively, through interaction via social media.
- Brute force – An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found.
- Denial of Service (DoS) – Prevents legitimate and authorized users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.
- Spear-phishing – Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.
- Subverting the supply chain – Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship. Above examples are not exhaustive as other methods are evolving such as impersonating a legitimate shore-based employee in a shipping company to obtain valuable information, which can be used for a further attack. The potential number and sophistication of tools and techniques used in cyberattacks continue to evolve and are limited only by the ingenuity of those organizations and individuals developing them.

Cyber threats can be classified into 2 categories – "External" and "Internal".

"External" threats include but are not limited to the following:

Table 2: "*External" threats classification*

Group	Motivation	Objective
Activists	*reputational damage *disruption of operations	*destruction of data *publication of sensitive data media attention
Criminals	*financial gain *commercial espionage industrial espionage	*selling stolen data *ransoming stolen data *ransoming system operability *arranging fraudulent transportation of cargo
Opportunists	*the challenge	*getting through financial cyber security defences *financial gain
states, state sponsored organisations, terrorists	*political gain *espionage	*gaining knowledge *disruption to economies and critical national infrastructure

"Internal" threats include but are not limited to the following:

Table 3: "*Internal" threats classification*

Group	Motivation
insecure systems	*unlocked equipment cabinets, offices or facilities *unattended user equipment
theft or equipment or data	*equipment or systems left unattended *inadequate security practises
impersonation of account	*weak passwords *loss of ID credentials *default admin account passwords
malicious software	*malware *outdated antivirus software
malfunctioning software	*unpatched software *inadequate change management process
restriction control violation	*inadequate access controls *inadequate security configuration
social engineering	*phishing attacks *ransomware

4. Qualification of the person responsible for companies' fleet cyber security

Effective cyber risk management relies on a clear allocation of responsibilities and tasks within the company. Cyber risk management is an integral part of ship management and ship operation, and different employees have different roles, responsibilities, and tasks. Furthermore, in some companies, some roles, responsibilities, and tasks are outsourced to third parties. The various responsibilities and tasks should be mapped to the job descriptions and/or role descriptions found in the SMS. As cyber risk management planning and execution involves the whole company it may be useful during the mapping process to clarify who is the responsible person, and who is required to support that person. For example, a ship IT manager may well be the responsible party for cyber risk management in ships, but he relies on support from other managers and staff from across the whole company, security staff, safety staff, training staff, procurement staff, marine HR staff, crew etc. Often, the allocation of responsibilities and tasks will work best if it is aligned with the normal chain of command. For example, when allocating the responsibility for compliance with cyber risk management procedures on board a ship, it will often make sense to appoint the Master or the Chief Engineer [3].

Cyber risk management should involve the senior management level of a company on an ongoing basis, instead of for example, only the ship security officer or the IT manager [4]. There are several reasons for this:

- Some cyber risks have wide-ranging destructive potential to the safety of personnel and the environment as well as the performance and reputation of the company. Cyber risks are therefore not simply security challenges, but business challenges that require leadership's involvement;
- Initiatives to heighten cyber security and safety may affect standard business procedures and operations by rendering them more time consuming and/or costly. It is, therefore, a senior management decision to evaluate and allocate the necessary resources to establish risk mitigation to an acceptable level of residual risk;
- Initiatives, which heighten cyber awareness, may change how the company interacts with unions, customers, suppliers, and authorities, and impose new requirements on the cooperation between parties. It is a senior management decision whether to drive these changes in relationships and how best to do so.

The answers to the following questions may be used as a basis for informing and involving senior management about the importance of addressing cyber risks onboard ships:

• What assets are at risk?
• What is the potential impact of a cyber incident to the business, customers, partners, and stakeholders?
• Who has the final responsibility for cyber risk management?
• Are the OT systems and their working environment protected from unauthorized access and changes?
• Is there remote access to the OT systems and, if so, how is it monitored and protected?
• Are the IT systems protected and is access being monitored and managed?
• What cyber risk management best practices are being used?

Based on the answers, the company should describe and delegate authority as appropriate, and allocate the resources needed to develop and maintain suitable solutions based on the risk assessment results.

Security Officer is the first line of defense against malicious actors in the IT industry. They screen their company's critical IT infrastructure for weaknesses and create robust countermeasures to prevent future incidents. Security Officer also train ship's crew on security best practices and advice management on investments to safeguard the company's and or ship's computer and network systems [5]. Here are examples of Security Officer responsibilities:

• Develop, execute and track the performance of security measures to protect information and network infrastructure and computer systems.
• Design computer security strategy and engineer comprehensive cybersecurity architecture.
• Identify, define and document system security requirements and recommend solutions to management.
• Configure, troubleshoot and maintain security infrastructure software and hardware.
• Install software that monitors systems and networks for security breaches and intrusions.
• Monitor systems for irregular behavior and set up preventive measures.
• Plan, develop, implement and update company's information security strategy.
• Educate and train staff on information system security best practices.

5. Conclusion

Is there any minimum requirements recommendation for the company to appoint person responsible for Companies' fleet cyber security and on board Cyber Security Officer? There is no requirement decided by the IMO. Competency requirements are found in the ISM Code and in the Maritime Labour Convention (Regulation 1.3). In my opinion there must be people with cyber security responsibility in the company and on board the vessels and communication between those persons to ensure ongoing compliance and continuous improvement. Despite that from the ISM Code it must be inferred that there has to be a person or persons on board responsible for handling the safety management systems measures on cyber security, from the ISM/statutory perspective no regulation for a ship cyber security officer (SCSO), his qualifications and trainings. That said, there are requirements from ISM and the MLC that staff shall be qualified for their tasks. This allows the shipping Company to develop and implement solutions (including through external providers) to handle their obligations.

References:

1. K. Hopcraft, *50,000 Ships worldwide are vulnerable to cyberattacks*, (2018) [Online] Available: https://www.independent.co.uk/tech/ships-cyberattacks-vulnerable-worldwide-a8404191.html
2. K. Kochetkova, *Maritime industry is easy meat for cyber criminals*, (2015) [Online] Available: https://www.kaspersky.com/blog/maritime-cyber-security/8796/?ref=555601-91802X1545674X0299c634135b24a95a598a642f1cfb7c&affmt=2&affmn=1
3. *Cyber-Security-Guidelines*, (2021) Version 4, Working Group BIMCO, Columbia Shipmanagement Cyprus (Chairperson), Chamber of Shipping of America, Digital Containership Association, Interferry, INTERMANAGER, International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Marine Contractors Association (IMCA), International Union of Marine Insurance (IUMI), Moran Cyber, Maersk, Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass), World Shipping Council. [Online] Available: https://www.ics-shipping.org/resource/guidelines-on-cyber-security-onboard-ships-version-four/
4. B. Belev, P*urdue model implementation in the shipping control systems*, (2022) 10th International Scientific Conference on Computer Science (COMSCI), 30 May-02 June, Sofia. DOI:10.1109/COMSCI55378.2022.9912594.
5. B. Belev, *Maritime education development for environment protection behavior in the autonomous ship's era*, (2019) Scientific Bulletin" Mircea cel Batran" Naval Academy 22 (1), 1-8