1 Safety Assessment “Cyber Security Hazards for Ship Owners”

Main hazard:	Cyber Security Hazards
Identified by:	Svensk Sjöfart
Time period looked at:	until June 2020
Cases identified/ of total in the database:	12/ 3757
Cases actively removed from search:	0
Author	Johannes Hüffmeier, RISE Research Institutes of Sweden
Date	2020-09-16

1.1 Trend Background

The IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

With an increase of IT systems, with the trends of automation, digitalization and IoT the threats connected to cyber-attacks increase in importance. Vessel navigation, cargo handling and maintenance systems on ships, cargo/ passenger handling and tracking systems in ports, are all controlled using software that is fundamental to smooth-running operations. If, for example, a cyber-attack disabled a vessel transiting in certain fairways like the Suez or Panama Canal, it could result in blockage of the channel affecting economies worldwide.

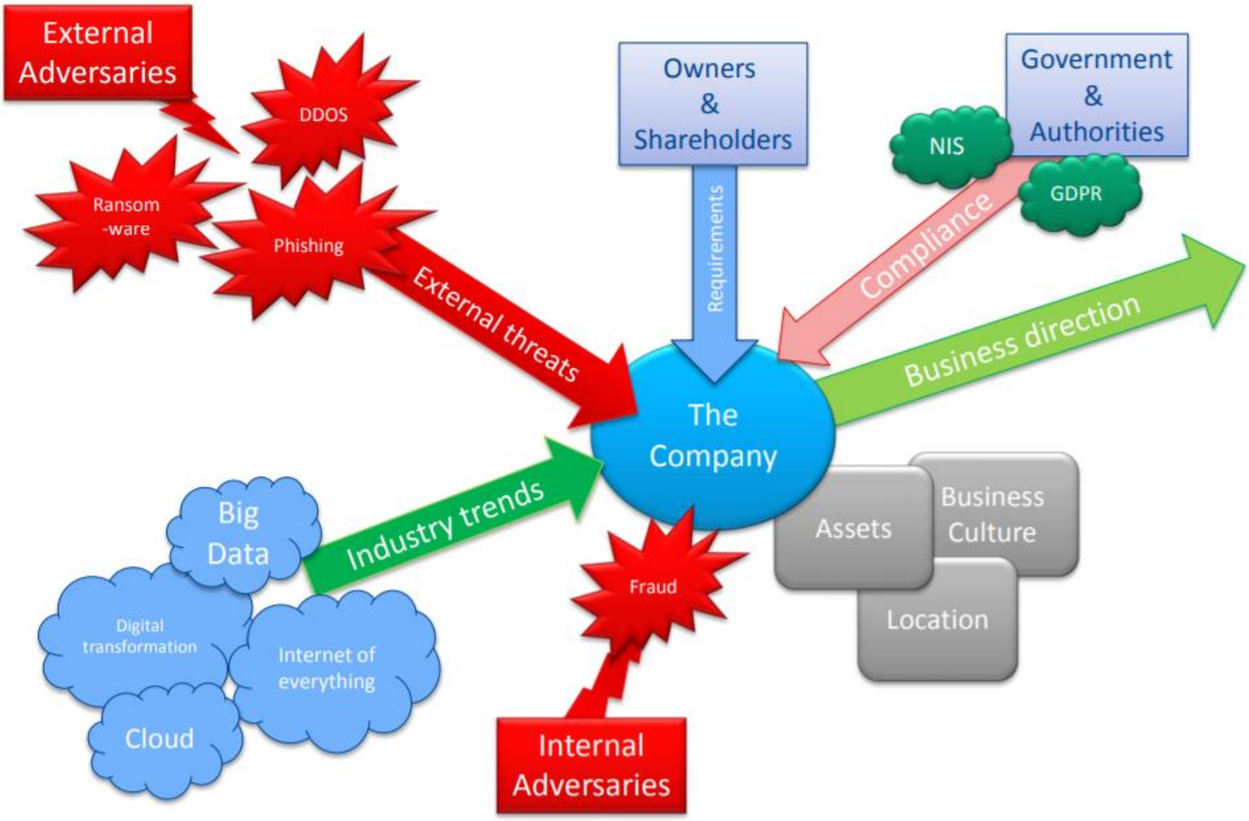

Figure 1: Threads to the Maritime Industry [1]

Figures from land show that 50% of incidents caused by incorrect configuration of the networks 23% of people open phishing mails, half of all people reuse passwords across work and private applications and 99% of breaches come from known vulnerabilities [1]. Hackers penetrating networks, and critical equipment could result in significant safety, downtime, financial and potential reputational damage.

Certain guidelines and standards have been established. DNV GL's Cyber Secure class notation establishes a baseline to identify cyber security levels for the main functions of a vessel, either in operation or during construction, and offers owners and operators a framework to improve and demonstrate their cyber resilience. [2]

The Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003, or a variant of that clause, has appeared on marine policies for the past 15 years, excluding any loss, damage, or liability caused either directly or indirectly by the use of a computer and its associated systems and software "as a means of inflicting harm." [4]

Cyber-attacks can be performed by different parties and with various methods.

- **Activists (including disgruntled employees/ passengers)** with the motivation of reputational damage and disruption of operations aim for destruction of data, publication of sensitive data, media attention and denial of access to the service or system targeted
- **Criminals** with the motivation of **financial gain, commercial espionage, industrial espionage** aim for selling stolen data, ransoming stolen data, ransoming system operability, arranging fraudulent transportation of cargo, gathering intelligence for more sophisticated crime, exact cargo location, ship transportation and handling plans etc.
- **Competitors** with the motivation of **financial gain, commercial espionage and industrial espionage** aim for using stolen data, gaining knowledge, get to know functions and architecture of components, etc.
- **Opportunists** with the motivation of the **challenge** as such aim for getting through cyber security defences and financial gain
- **States/ State sponsored organisations/ Terrorists** with the motivation of political gain and espionage aim for gaining knowledge and disruption to economies and critical national infrastructure
- **Disgruntled Employees** with the motivation of **revenge** aim for financial harm to the companies involved

1.2 Hazard Identification

The hazard identification is not directly based on the trend and the resulting searched events in Foresea. No cyber-attacks have been reported. Only security breaches have been collected from the system which could have resulted in physical based cyber-attacks. The Ishikawa / fishbone diagram provides basic information on the event, the causal factors and the consequences. Most of the cases originate to **security breach**. Causes that relate to humans and manning are found as **criminal actions,** causes related to management are mainly categorized by **Supervision/ Responsibility** while working environment causes can be found in **protection devices and safeguards**. Other causal contributors are found in the yard/ port/ terminal interface.

Consequences according to the fishbone diagram are dominated by mental strain for the crews, **Time Loss/ Delay/ Deviation** and **Machinery/ Equipment damage.)** Ships affected by attacks can be out of control because of these problems can cause extensive damage to shipping companies, crews and assets.

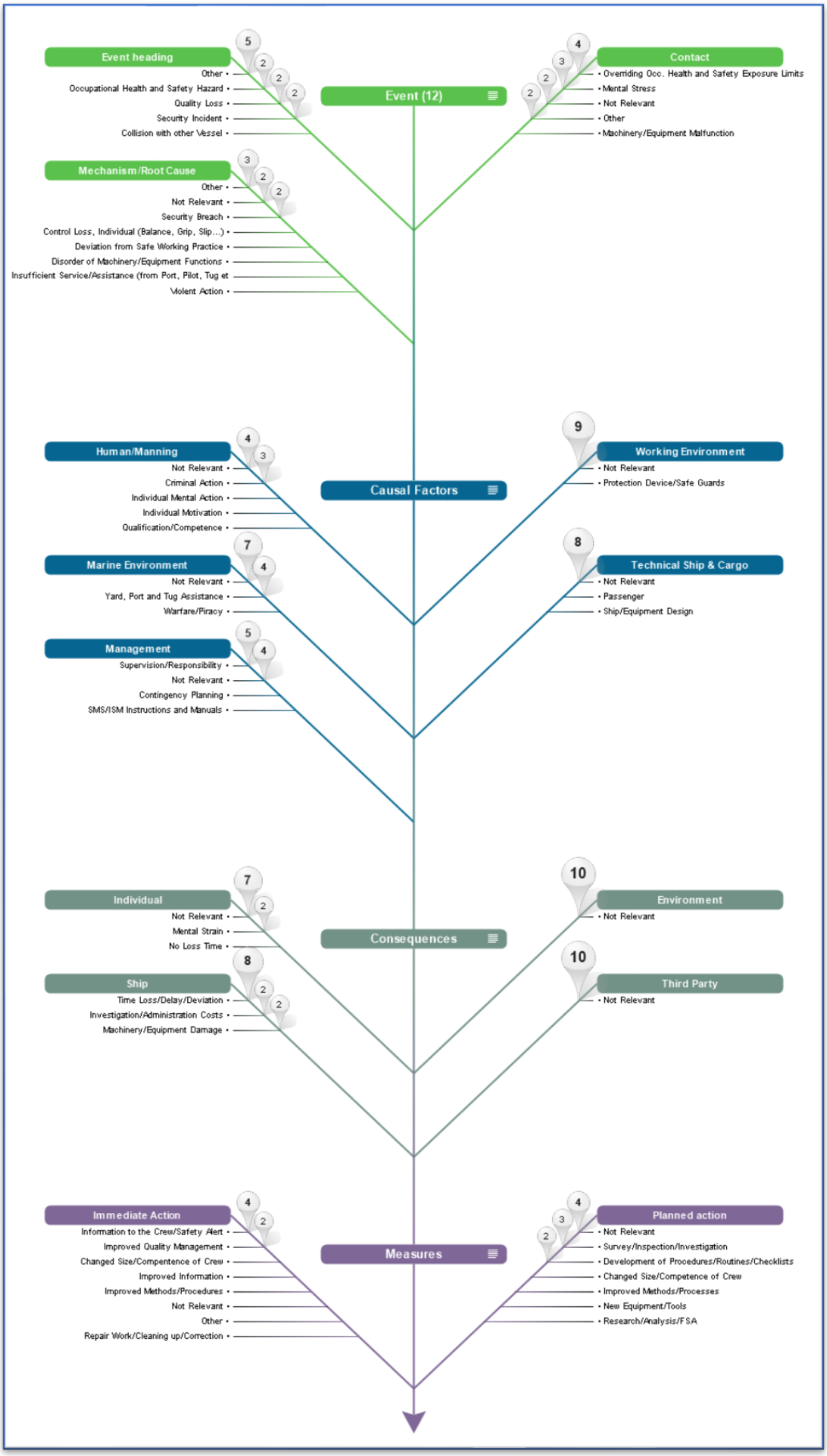
Event heading
5
2
2
2
Other
Occupational Health and Safety Hazard
Quality Loss
Security Incident
Collision with other Vessel
Event (12)
Contact
4
3
2
2
Overriding Occ. Health and Safety Exposure Limits
Mental Stress
Not Relevant
Other
Machinery/Equipment Malfunction
Mechanism/Root Cause
3
2
2
Other
Not Relevant
Security Breach
Control Loss, Individual (Balance, Grip, Slip...)
Deviation from Safe Working Practice
Disorder of Machinery/Equipment Functions
Insufficient Service/Assistance (from Port, Pilot, Tug et
Violent Action
Human/Manning
4
3
Not Relevant
Criminal Action
Individual Mental Action
Individual Motivation
Qualification/Competence
Causal Factors
Working Environment
9
Not Relevant
Protection Device/Safe Guards
Marine Environment
7
4
Not Relevant
Yard, Port and Tug Assistance
Warfare/Piracy
Technical Ship & Cargo
8
Not Relevant
Passenger
Ship/Equipment Design
Management
5
4
Supervision/Responsibility
Not Relevant
Contingency Planning
SMS/ISM Instructions and Manuals
Individual
7
2
Not Relevant
Mental Strain
No Loss Time
Consequences
Environment
10
Not Relevant
Ship
8
2
2
Time Loss/Delay/Deviation
Investigation/Administration Costs
Machinery/Equipment Damage
Third Party
10
Not Relevant
Immediate Action
4
2
Information to the Crew/Safety Alert
Improved Quality Management
Changed Size/Compentence of Crew
Improved Information
Improved Methods/Procedures
Not Relevant
Other
Repair Work/Cleaning up/Correction
Measures
Planned action
4
3
2
Not Relevant
Survey/Inspection/Investigation
Development of Procedures/Routines/Checklists
Changed Size/Competence of Crew
Improved Methods/Processes
New Equipment/Tools
Research/Analysis/FSA

Figure 2: Physical security breaches reported to Foresea

1.3 Risk assessment

Cyber-attacks can be made by either a person physically onboard, or more often by remote attacks. It is typically differentiated between two different types of attacks, that could affect companies and ships:

- untargeted attacks, where systems and/ or data are one of many potential targets
- targeted attacks, where systems and/ or data are the intended target.

Little is published on cyber-attacks publicly. Known attacks are listed in the table below. Figures of probability of attacks are in the order of magnitude 1,000,000 events/day/vessel, ~ 11,000 cyber threats and 80% conducted from crew network where ~97% of malware is designed to exploit social engineering weaknesses, not a technical flaw. [5]

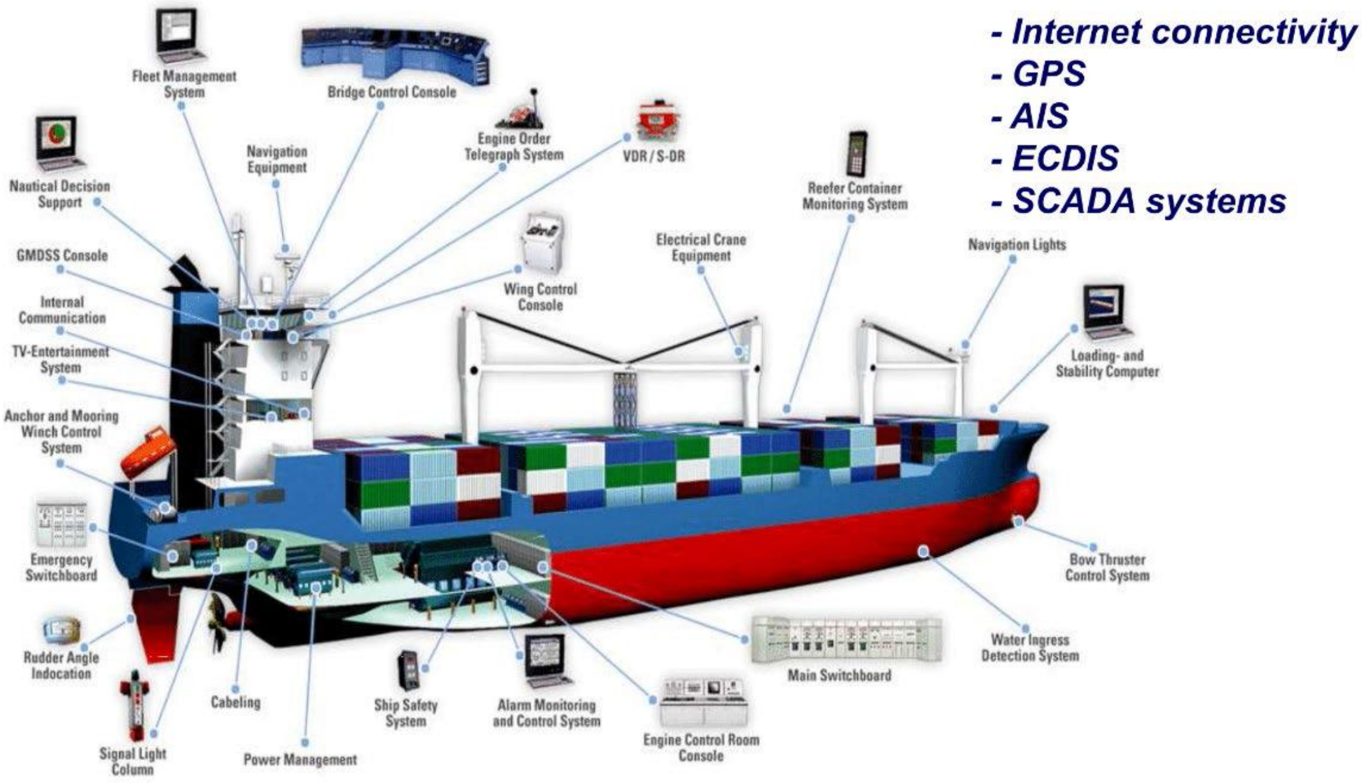

Figure 3: Systems on a ship exposed to cyber threads [5]

Besides the cases listed below, various attacks on GPS and AIS have been executed, such as spoofing, jamming, replay, etc.

Date	Victim
2010-11	Greek Shipping Company
Aug 2011	Iranian Shipping Line (IRISL)
2011-13	Port of Antwerp
2012	Australian Customs and Border Protection Service agency
2012-14	Danish Port Authority
Apr 2016	South Korea
Jun2017	AP MollerMaersk
Jun 2017	Ships in Novorossiysk
Nov 2017	Clarksons
July 2018	Cosco US

Date	Victim
Sep 2018	Ports of Barcelona & San Diego
2018	The Jerusalem Post. (2018, October) Avoiding detection: The team tracking Irans attempt to cloak its oil exports. Available: https://www.jpost.com/Middle-East/Avoiding-detection-Theteam-tracking-Irans-attempt-to-cloak-its-oil-exports-570236
2013	InsideGNSS. (2013, April) North koreas GPS jamming prompts south korea to endorse nationwide eloran system. [Online]. Available: https://insidegnss.com/north-koreas-gps-jamming-promptssouth- korea-to-endorse-nationwide-eloran-system/
2018	Business Insider Australia. (2018, April) China has jamming equipment in the south china sea – and the US may 'not look kindly on it'. [Online]. Available: https://www.businessinsider.com.au/chinajamming-us-navy-jets-off-aircraft-carriers-pacific-2018-4
2018	GPS World. (2018, November) GPS disrupted for maritime in Mediterranean, Red Sea. [Online]. Available: https://www.gpsworld.com/gpsdisrupted-for-maritime-in-mediterranean-red-sea/

Table 1: Publicly available information on cyber-attacks in the maritime industry

Cyber attacks can be on large and on small scale. Often, an opener for cyber attacks builds upon daily work of the crews. Typical threats identified affecting crews' everyday activities onboard are connected to [2]:

- Repair broken IT equipment
- Install software
- Patch/update software
- Install new hardware
- Buy new hardware
- Change physical IT infrastructure
- Allow 3rd party people to access and modify the IT setup
- Use shore based WiFi

Consequences can have very different character and impact. While the Maersk attack was very costy and interrupted operations worldwide, other conseuqnces can be more locally or limited to single systems. In worst case scenarios, ship systems may be compromised, resulting in

1. operational interruption
2. pollution
3. loss of cargo
4. physical injury to crew
5. loss of or damage to ships

1.4 Risk-Reducing Measures and Cost-Benefit Analysis

Typical frameworks used in the context of cyber security follow the NIST Framework (National Institute of Standards and Technology) as shown in the figure below. While the response to cyber security attacks is the consequence reducing measure, most of the work on cybersecurity is built upon the preventive measures made in single organisations and as a joint effort in the whole shipping industry.

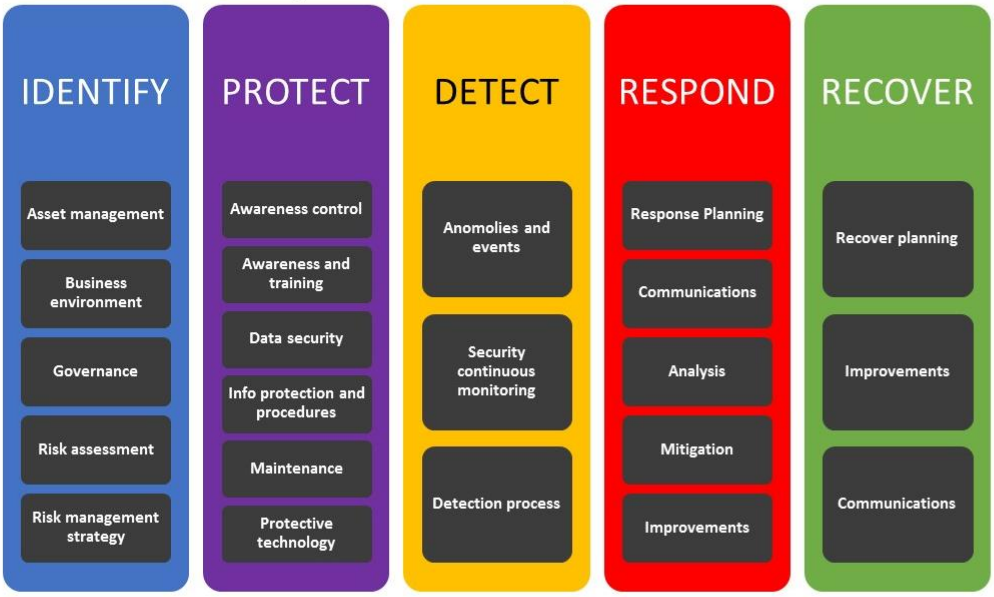

Figure 4: NIST framework on cyber security

The main difference when it comes to risk reducing measures is made by an increased awareness on cyber security issues in the whole organization, as described in the picture below from BIMCOS guidelines. [6]

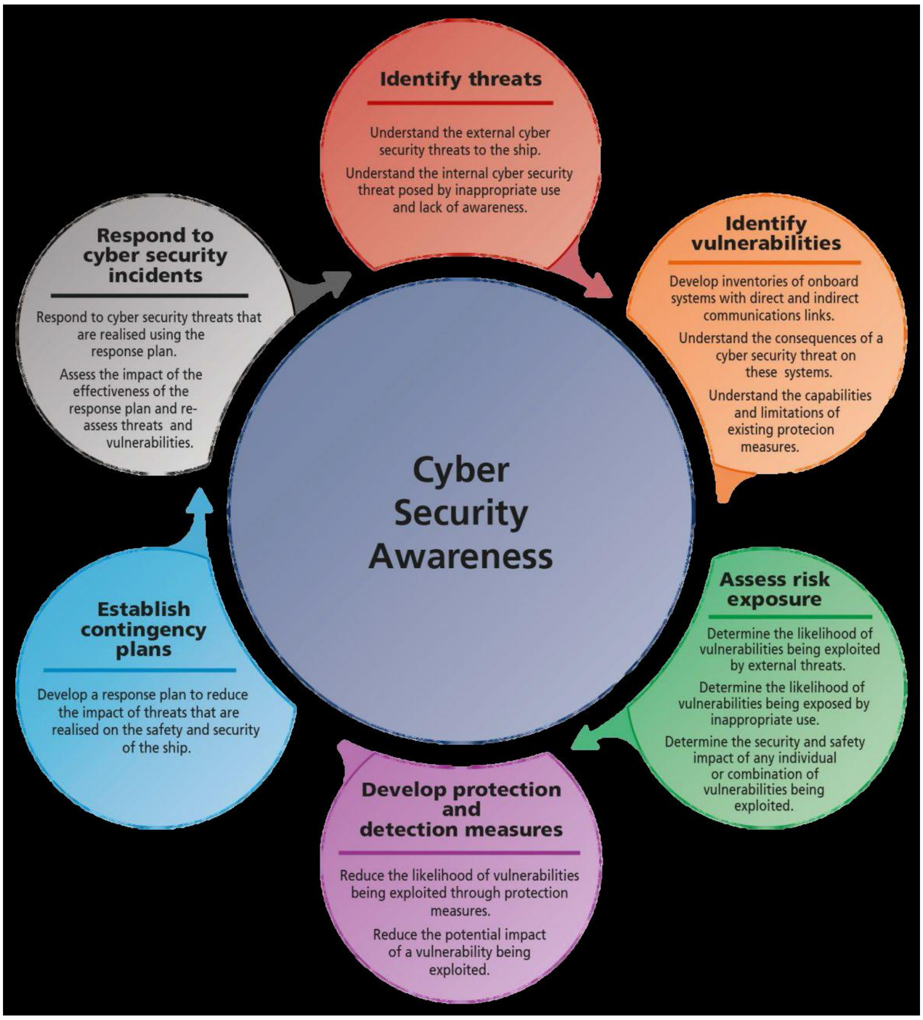
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness

Figure 5: Cyber Security Awareness [6]

Relevant security measures identified can be categorised into three different groups: Policies, Organisations, and technology. [7]

POLICIES

- Security policy and organization
- Risk and Threats Management
- Security and privacy by design
- Asset inventory and management
- Cyber resilience (Business continuity and crisis management)

ORGANISATIONAL PRACTICES

- Endpoints protection and lifecycle management
- Vulnerabilities management
- Human Resource Security
- Supply chain management
- Detection and Incident response
- Control and auditing
- IT and OT physical protection

TECHNICAL MEASURES

- Network security
- Access control
- Administration and Configuration Management
- Threat management
- Cloud security
- Machine-to-machine security
- Data protection
- Update management
- Detection and monitoring
    - Industrial control systems security
    - Backup and restore

1.5 Conclusions and Recommendations for Decision-Making

There is no single solution to managing cyber threats. Cyber risk management should be an inherent part of the safety and security culture conducive to the safe and efficient operation of the ship and be considered at various levels of the company, including senior management ashore and onboard personnel. In the context of a ship's operation, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. [5]

Company plans and procedures contained in the ISM Code and ISPS Code should incorporate cyber risk management into existing security and safety risk management requirements.

A systematical analysis of the cyber threats should be performed, following the steps described below, following a typical risk assessment approach:

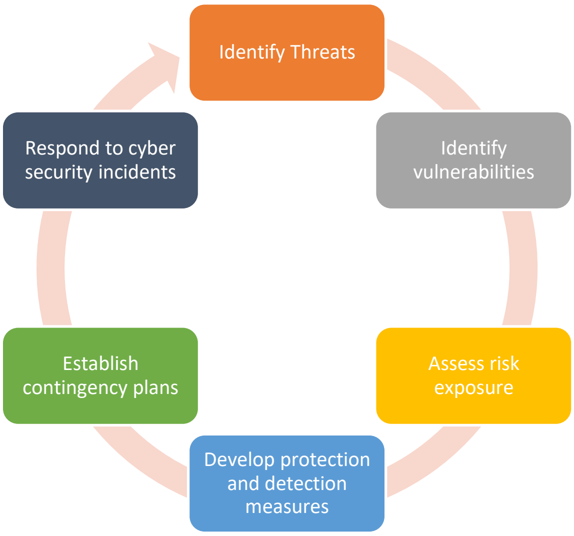
Identify Threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond to cyber security incidents

Figure 6: Constant activities towards cyber security

Basic work for shipping companies shall consist of increased awareness of the realistic threat picture by performing realistic Cyber Security Assessment. The companies need to develop contingency plans as well as countermeasure plans and need to regularly work on training and awareness at all levels onboard and ashore.

References

[1] M. Carling, *The Convergence of Risks,* Stockholm: Stena AB, Transportstyrelsens Sjöfartsseminarium, 2018.

[2] L. Jensen, *Maritime Cyber Risks, What is reality and what is hype?- Where should we focus?,* Mariehamn/ Åland: CyberKeel, Maritime Day Åland, 2018.

[3] N. Späth, "Stena Drilling and DNV GL sign contract for first Cyber Secure class notation," DNV GL, 04 April 2019. [Online]. Available: https://www.dnvgl.com/news/stena-drilling-and-dnv-gl-sign-contract-for-first-cyber-secure-class-notation-149153.

[4] MARSH, *The Risk of Cyber-Attack to the Maritime Sector,* London: Marsh - Global Marine Practice, 2014.

[5] C. Kapalidis, *Cyber Risk Management for the Maritime Sector,* London: Hudson Analytix, Chatham House, 2018.

[6] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, *The Guidelines on Cyber Security Onboard Ships,* Copenhagen: BIMCO, 2018.

[7] D. A. Drougkas, A. Sarri, P. Kyranoudi och A. Zisi, *PORT CYBERSECURITY - Good practices for cybersecurity in the maritime sector,* ENISA: Athens, 2019.