Guidelines of Maritime Cybersecurity for Ships in Indonesian Waterways from a Classification Society Point of View

M. Rizqi Hariadi and Rizky Prasetya Ade Nugroho
PT. Biro Klasifikasi Indonesia, Indonesia

Keywords: Cybersecurity, Guidelines, Assessments, Classification Society.

Abstract: Indonesia is ranked the 4th largest in the growth of internet users in the world. This growth brings positive impact that is increasing Indonesia's opportunities in developing digital and internet technology. However, this growth also subjected Indonesia to increasing digital threat. To combat this threat, cybersecurity is implemented which consists of technologies, processes, and measures designed to protect networks, devices, programs, and data from threat such as attack or unauthorized access. On maritime sector, cybersecurity is one of element of safety that is regulated in ISM (International Safety Management) code and is therefore mandatory to be fulfilled by ship owners. As Indonesia's only national classification society, it is BKI's responsibility to ensure Indonesian ship's safety, including their cybersecurity aspect. One of the ways to do that is by providing guidelines that can be used by ship owners to implement cybersecurity in their respective organization. This paper will explain the development process of BKI's cybersecurity guidelines which involves gap analysis of existing cybersecurity guidelines and their implementation in the context of maritime sector. Subsequently, this paper will also briefly explain the content of the guidelines.

1 INTRODUCTION

Industry 4.0 brings big impact to industry sector, an impact that also influences Indonesia as a country that is ranked the 4th largest in the growth of internet users in the world. This growth brings positive impact that is increasing Indonesia's opportunities in developing digital and internet technology. However, this growth also subjected Indonesia to increasing digital threat. Based on 2020 Global Cybersecurity Index by International Telecommunication Union (ITU), Indonesia's global index is ranked the 24th from 182 countries in the world (ITU, 2021), while according to annual report of BSSN (Badan Siber dan Sandi Negara), there were 1.6 million cyber-attacks in Indonesia in the period of time from 1 January to 31 December 2021. The BSSN annual report also shows that 46.6% of the attack is Botnet type (Laptah, 2021) which is a computer network that is infected with malware and under the control of attacker.

Cybersecurity consists of technologies, processes, and measures designed to protect networks, devices, programs, and data from attack or unauthorized access. Cybersecurity can also be thought as information security technology. Cyber-attack commonly consists of several stages, which are collecting information from target organization/entity, scanning to search for security hole in a system, acquiring access illegally, maintaining access to copy data or destroy the system and covering tracks to avoid detection. In maritime world, cyber-attacks can be categorized into two category, cyber-attacks targeting the ship and cyber-attack targeting sectors supporting maritime world, for example ports. In the period of 1 year from 2010 to 2011, shipping companies in Greece had suffered eleven pirate attack in Somalia, eight of which had their voyage schedule and cargo data leaked to unauthorized party through security hole in wi-fi connection as a consequence of wireless lamp installation (Chalermpong senarak, 2021). This case indicates that while technological advancement can bring many opportunities, it can also bring new kinds of risks as well.

To combat this growing threat, cybersecurity needs to be implemented. Cybersecurity consists of technologies, processes, and measures designed to protect networks, devices, programs, and data from threat such as attack or unauthorized access. In maritime world, International Maritime Organization (IMO) has already made cybersecurity element

Hariadi, M. and Nugroho, R.
Guidelines of Maritime Cybersecurity for Ships in Indonesian Waterways from a Classification Society Point of View.
DOI: 10.5220/0012008500003575
In *Proceedings of the 5th International Conference on Applied Science and Technology on Engineering Science (iCAST-ES 2022)*, pages 1012-1017
ISBN: 978-989-758-619-4; ISSN: 2975-8246

mandatory in International Safety Management (ISM) code since 1 January 2021.

The ISM code itself is one of statutory matter whose implementation depends on national regulation where the ship is registered. To ensure that the ships comply to ISM code and any other regulation that may applicable, inspection is done which is carried on by government agency. In Indonesia's case, this inspection is carried on by Ministry of Transportation or other organization that may represents Government of Indonesia to carry on the inspection which is called Recognized Organization (RO). One such organization is Biro Klasifikasi Indonesia (BKI).

BKI is Indonesia's only national classification society. It is BKI's responsibility to ensure Indonesian ships follow standards that will increase their safety. Since BKI also acts as Indonesia's RO, it may represent Government of Indonesia in inspecting ships' compliance with national regulations and statutory matters including ISM code which in turn also includes cybersecurity element. To help ship owners comply with the cybersecurity requirements, BKI has published guidelines to implement cybersecurity named Guidelines for Maritime Cybersecurity. The subsequent sections will explain the methodology used to develop the guidelines and also briefly explain the contents of Guidelines for Maritime Cybersecurity.

2 METHODOLOGY

In developing the Guidelines for Maritime Cybersecurity, BKI conducts gap analysis from several references such as class partner guidelines and international standards. After gap analysis is performed, the standards are analyzed further to determine which requirements are viable to be implemented in Indonesia. The aspects considered are notation, cybersecurity development methodology and classification scope.

3 RESULTS AND DISCUSSION

As mentioned in previous section, gap analysis is performed to several cybersecurity standards such as class partners' guidelines and international standards. The standards reviewed are NIST Cybersecurity Framework, IMO MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management, and cybersecurity guidelines from Det Norske Veritas (DNV), China Classification Society (CCS), Indian Register (IRS), Lloyd's Register (LR Class) and American Bureau of Shipping (ABS).

3.1 NIST Cybersecurity Framework (2018)

This is a framework for implementing cybersecurity on general system that is published by The National Institute of Standards and Technology (NIST). The core of this framework comprises of four elements that is Functions, Categories, Subcategories and Informative References. Functions, as the highest level of the elements, defines the basic cybersecurity activity and consist of:

- Identify
- Protect
- Detect
- Respond
- Recover

The framework also defines 4 tiers that categorizes an organization implementation of the framework. These tiers are Tier 1 – Partial, Tier 2 – Risk Informed, Tier 3 – Repeatable and Tier 4 – Adaptive. Although very detailed, this framework targets general system and may need several adjustments to be applied specifically in maritime context.

3.2 IMO MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management

This Guidelines is published by IMO to provide high level recommendations on maritime cyber risk management. As such, these guidelines do not provide detailed requirements on how to implement cybersecurity in ships or organizations. The user is instead directed to other additional guidelines for detailed implementation of cyber risk management. At its core, these guidelines present the same functional elements that is explained in NIST framework, that is Identify, Protect, Detect, Respond and Recover.

3.3 DNV (2016)

The Guidelines published by DNV is developed based on references from BIMCO and IMO guidelines. The aim of these guidelines is to provide set of requirements that can be used by enterprise to measure their cyber risk level, develop cybersecurity implementation and verify that the developed system is running appropriately.

In these guidelines, assessment is divided into three levels, high level assessment, focused assessment and comprehensive assessment. High level assessment is the first stage of improving enterprise cybersecurity and conducted by senior management. The focus of this stage is mainly technical aspect, cybersecurity awareness, policy and cybersecurity implementation. Output of this stage is cyber risk matrix.

The second stage, focused assessment, is conducted by staffs with knowledge of IT, industrial control/automation and risk methodology. In this stage, threat to system is identified, barrier to prevent the attack is planned and means to minimize risk of threat is defined. Afterwards, assessment is done to measure the impact of barrier weakening and the means to prevent such cases.

Comprehensive assessment is performed based on ISO/IEC 27001. In this stage, consequence of successful cyber-attack is assumed which focused on confidentiality, integrity, availability and authenticity. The output of this assessment is improvement related to technical aspect and security management.

3.4 CCS (2020)

These Guidelines mainly explains about implementation of cybersecurity onboard ships. Focus of these guidelines is construction, operation, maintenance and survey process of ships that implements cybersecurity. There are two kind of notation assigned to ships that comply with the requirements of these guidelines that is P and S. P notation denotes the lowest level of requirement, while S notation is given to ships that comply with highest level of requirements in these guidelines. This guidelines uses references from IACS UR E22, IEC and CCS own rules. Types of survey for ships with cybersecurity notation is the same with any other ships that is annual, intermediate and special survey. The scope of the surveys is inspection and assessments regarding ship cybersecurity requirements and their management.

3.5 IRS Class (2017)

The IRS guidelines focus on implementation of cybersecurity on board the ship and shore-based facility. Notations given to ships that comply with these guidelines are divided into 3 categories, CyS-I, CyS-II, dan CyS-III. The roman numeral denotes the level or complexity of the requirements and their corresponding inspection where roman numeral I is the lowest level and III is the highest level. In these guidelines, for ships that is assigned with CyS notation, their corresponding shore-based facility can be awarded similar notation with additional qualifier as per owner request.

3.6 LR Class (2017)

The guidelines published by LR class also focus on cybersecurity on board the ship. The subject of these guidelines is type of ship that is categorized by these guidelines as “cyber enabled” – ships with on board IT and OT system which is controlled conventionally by crew or autonomously without crew. Assignment of ship notation in these guidelines is divided into two broad categories as follows:

- Cyber Functionality
  This notation is further divided into 4 categories as follows:
  - Cyber safe: essential system in ship operation that has remote access to onboard ship operational data has proven to be secure
  - Cyber maintain: maintenance system in ship that has remote access to onboard ship operational data has proven to be secure
  - Cyber perform: optimization system in ship that has remote access to onboard ship operational data has proven to be secure
  - Cyber secure: remote access in ship has proven to be secure
- Cyber Assessment
  This notation is further divided into 6 categories as follows:
  - AL 0: no cyber access, no assessment is needed
  - AL 1: manual cyber access, no assessment is needed
  - AL 2: cyber access is used only for autonomous/remote monitoring
  - AL 3: cyber access is used for autonomous/remote monitoring and control (onboard permission required)
  - AL 4: cyber access is used for autonomous/remote monitoring and control where onboard permission is required and onboard override is possible
  - AL 5: cyber access is used for autonomous/remote monitoring and control where onboard permission is not required and onboard override is not possible

3.7 ABS Vol. I dan II (2016)

ABS Guidelines is divided into 2 volumes where volume I focuses on cybersecurity management, while volume II deals with ship notations and their respective inspection items. Generally, cybersecurity management explained in these guidelines is similar to other guidelines that has been reviewed. The difference lies only on the terms used. Class notation that assigned to the ship is divided into 3 types, CS 1 (basic cybersecurity), CS 2 (developed cybersecurity) and CS 3 (adaptive cybersecurity). These notations can be assigned flexibly, for example when a ship is requested to be assigned with CS 1 notation but it is able to satisfy some requirements of CS 2, the ship will be awarded CS 1 notation with additional requirement form CS 2.

3.8 Key Points

From the review of 7 guidelines, it can be concluded that cybersecurity management can be implemented by following the general steps as follows:

1) Enterprise cybersecurity design and planning
2) Implementation of the system
3) Review of cybersecurity performance especially in withstanding cyber attack
4) Responding to cyber-attack or threat according to design
5) Improving cybersecurity management, not only in technical aspect but also in awareness and human aspect

3.9 BKI Guidelines for Maritime Cybersecurity

Based on analysis result, BKI has developed Guidelines for Maritime Cybersecurity whose outlines is shown in table 1.

Table 1: Outline of BKI Guidelines for Maritime Cybersecurity.

Section	Name
Section 1	General
Section 2	Cybersecurity Program Development
Section 3	Cybersecurity Management System
Section 4	Requirement for cybersecurity system
Section 5	Surveys and maintenance of class

Section 1 explains the scope of the guidelines. This section also defines the target of these guidelines that is ships and offshore facilities. Regarding the ships, these guidelines is applicable to both new building and existing ships. Class notation that will be assigned to ships complying with requirements in these guidelines also explained briefly and can be seen in Table 2 Matrix of application.

Table 2: Matrix of application.

Object	Notations (CS-1, CS-2, CS-3)	CC	CSC	Statement of fact
Shore facilities		X		
Management systems (ship/offshore)			X[1]	X[3]
Ship or offshore BKI classed	X		X[2]	X[3]
Ship or offshore non-BKI classed				X

1 Including information of cybersecurity level applied by the company (informed, advance, adaptive)
2 If the ship is found to comply with the CS notations, the CSC will be given to the operating company.
3 The statement of fact and/or assessment report may be issued by BKI upon requested by owner.

Aside from class notation (**CS-1, CS-2, CS-3**) there are other outputs of this guidelines, **CC** (Cybersecurity Certificate) that will be given to shore facilities and **CSC** (Cybersecurity Ship Certificate) that can be given to ship/offshore facilities or their corresponding management system. Furthermore if the owner does not request notation for the ships even though the ship itself already comply with the requirement of these guidelines, **Statement of Fact** can be issued by BKI, stating that the ship or facility has already comply with the requirements in BKI Guidelines for Maritime Cybersecurity. The flow of process from assessment request until issuance of notation or statement of fact can be seen on figure 1.

It is shown on Fig.1 that assessment request can come from ship owners, company or other related parties. The first step of assessment is review of FSD (Functional Specification Document) and CSMP (Cybersecurity Management Plan). Afterwards, risk assessment, cybersecurity management system assessment and risk profile development will be conducted. The last step of assessment process is capability assessment. After all step has been performed, the product can be issued, in the form of notation, Statement of Fact, CSC, or CC.

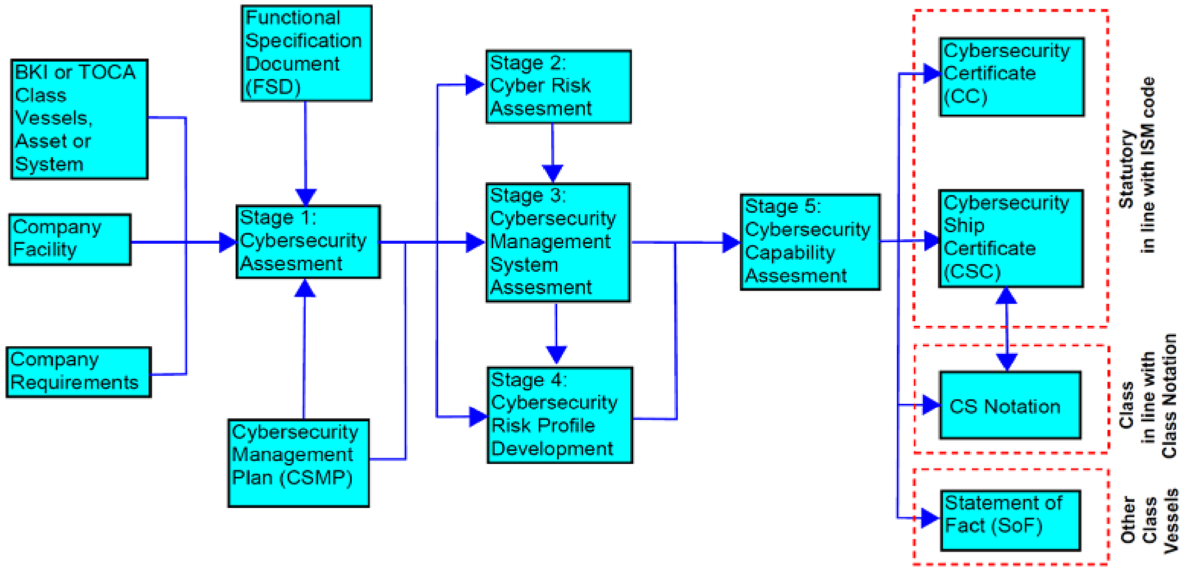
BKI or TOCA Class Vessels, Asset or System
Company Facility
Company Requirements
Functional Specification Document (FSD)
Stage 1: Cybersecurity Assesment
Cybersecurity Management Plan (CSMP)
Stage 2: Cyber Risk Assesment
Stage 3: Cybersecurity Management System Assesment
Stage 4: Cybersecurity Risk Profile Development
Stage 5: Cybersecurity Capability Assesment
Cybersecurity Certificate (CC)
Cybersecurity Ship Certificate (CSC)
CS Notation
Statement of Fact (SoF)
Statutory in line with ISM code
Class in line with Class Notation
Other Class Vessels

Figure 1: Cybersecurity admission flow of process (BKI Guidelines, 2021).

Section 2 Cybersecurity Program Development discusses about development of cybersecurity in a company. The main element of cybersecurity refers to functional elements of NIST Framework, that is:

- Identify
  Company must define key elements (personnel roles and responsibilities, asset, data, and capability), which expose company to high risk when affected by cyber-attack
- Protect
  Implementation of risk management and backup plan in case of cyber-attacks
- Detect
  Developing and implementing early detection of cyber-attack periodically
- Respond
  Establishing plans or measures to mitigate the risk of cyber-attacks that can hinder the operation of system/ship
- Recover
  Establishing plan to restore data or assets in case of successful cyber-attack

Section 3 Cybersecurity Management System discusses about steps that must be taken by company to maintain cybersecurity plan and development and ensures it is running as planned.

The detailed explanation for notations assigned to ship complying with these guidelines and their respective requirements are discussed in Section 4 Requirements for Cybersecurity System. There are 4 notations that can be assigned to ships as follows:

- **CS-1** (Informed Cybersecurity)
- **CS-2** (Advanced Cybersecurity)
- **CS-3** (Adaptive Cybersecurity)

where the CS-1 notation denotes the lowest level of cybersecurity while CS-3 is the highest. To be assigned with a notation, it is mandatory for the ship to also comply with all the requirements of the notation with lower level. For example, for a ship to be assigned with CS-2 notation, it must also comply with the requirements of CS-1 notation. Consequently, the ship with CS-3 notation must comply with all CS-1, CS-2 and CS-3 notations requirements.

Finally, Section 5 Surveys and Maintenance of Class discusses about the required surveys for class with CS notation. Generally, survey activities for these ships is the same with periodical survey of class (annual, intermediate, or special). Testing and inspection of cybersecurity functions can be done onboard the ships or offshore facilities.

4 CONCLUSIONS

Ships owners whose aware to protect their assets from cyber-attacks, can develop their own cybersecurity management based on BKI Guidelines for maritime cybersecurity, where divided into 3 level:

- **CS-1** (Informed Cybersecurity)
- **CS-2** (Advanced Cybersecurity)
- **CS-3** (Adaptive Cybersecurity)

These guidelines not only covers cybersecurity onboard ships but also cybersecurity for organization/company.

REFERENCES

ITU Publications (2021), Global Security Index 2020

BSSN, Laporan Tahunan Monitoring Keamanan Siber (2021)

ChalermpongSenarak (2021). The Asian Journal of Shipping and Logistics, 37 2021 20-36

NIST (2018). Cybersecurity framework ver.1.1

IMO (2017). MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management

DNV-GL (2016). RP-0496 Cyber security resilience Management for ships and mobile offshore units in Operation

CCS (2020). Guidelines for Requirement and Security Assessment of Ship Cyber System

IRS Class (2017). Guidelines on Maritime Cyber Safety

ABS Vol.I (2016). The Application of Cybersecurity Principles to Marine and Offshore Operations

ABS Vol.II (2016). Cybersecurity Implementation for The Marine and Offshore Industries

BKI (2021). Guidelines for Maritime Cybersecurity