World Maritime University

The Maritime Commons: Digital Repository of the World Maritime University

World Maritime University Dissertations | Dissertations

10-31-2021

A study on the vulnerability of Korean shipping companies to cybersecurity threats

Sungjae Kim

Follow this and additional works at: https://commons.wmu.se/all_dissertations

 Part of the Transportation Commons

This Dissertation is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact library@wmu.se.

WORLD MARITIME UNIVERSITY
Malmö, Sweden

A STUDY ON THE VULNERABILITY OF KOREAN SHIPPING COMPANIES TO CYBERSECURITY THREATS

By

SUNG-JAE KIM
Republic of Korea

A dissertation submitted to the World Maritime University in partial fulfilment of the requirements for the reward of the degree of

MASTER OF SCIENCE
in
MARITIME AFFARS

(MARITIME SAFETY AND ENVIRONMENTAL ADMINISTRATION)

2021

Copyright KIM, SUNG-JAE, 2021

Declaration

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature): **.....**

(Date): **.....**

Supervised by: Professor Raphael Baumler
World Maritime University

Supervisor's affiliation: Maritime Safety and Environmental Administration

Acknowledgements

First of all, I would like to thank the Government of the Republic of Korea for providing me an opportunity to increase knowledge and expand experience in the maritime field at the World Maritime University (WMU) in Malmö, Sweden. And I also express my sincere gratitude to Professor Raphael Baumler, who provided important advice and guidance in writing my dissertation successfully, and Mrs. Rebecca Sheehan, who has always helped me with kindness and careful consideration. Also, I would like to thank the WMU staff and faculty members for their various help and supports during my study at WMU.

I would also like to express my sincere gratitude to the staff members of the shipping companies, Korean Register, and the Korea Ship Managers Association for their willingness to participate in the dissertation survey despite their busy work.

And I would like to present my sincere thankfulness to my mother, father-in-law, and mother-in-law, who always gave me faith and love while worrying about my first foreign life.

Lastly, I would like to express my sincere love and gratitude to my wife Yoo Hee-young, who did not hesitate to give her own sacrifice and love to support my graduate school studies and to take care our lovely children, Kim Doo-hyun and Chae-young in a foreign country where COVID-19 is prevalent.

Abstract

Title of Dissertation: **A Study on the Vulnerability of Korean shipping companies to Cybersecurity Threats**

Degree: **Master of Science**

This dissertation is intended to evaluate the cybersecurity vulnerabilities of shipping companies and analyze their causes. In addition, based on the analysis results, this dissertation drew some recommendations on the policy direction for strengthening the cybersecurity of the International Maritime Organization (IMO) and member states.

Korean shipping companies were relatively well implementing 27 major cybersecurity elements derived from cybersecurity guidelines such as BIMCO and ISO/IEC. However, it was found that the group of small shipping companies was more vulnerable than the group of large shipping companies due to the wide variation of each company.

By analyzing the correlation between the company's cybersecurity vulnerabilities and various characteristics of the company, it was found that the company's cybersecurity capabilities, such as the company's organization and human resources, employee expertise, education, and training about cybersecurity, had the most remarkable correlation.

As a result of this analysis, it was suggested that IMO or member countries clarify the targets of policies related to cybersecurity, concisely and clearly present cybersecurity elements that companies should comply with, and consider cybersecurity from the time of designing ships.

KEYWORDS: cybersecurity, cybersecurity threat, cybercrime, cybersecurity elements, cybersecurity manager, shipping company, vulnerability, risk, risk assessment, correlation, Pearson correlation coefficient, coefficient of determination

Table of Contents

List of Tables

List of Figures

Introduction

1.1. Background

The impact of cybercrime on the global economy continues to increase due to the universalization of the Internet and smartphones, the strengthening of IT devices' connectivity by Cloud services and IoT devices. Cybersecurity firm McAfee and Centre for Strategic and International Studies (CSIS) reported global cybercrime costs up to $600bn in 2017, which increased up to 34% from $445bn in 2014 (as cited by Warwick, 2018).

Despite the rapid issue of cybercrime on land, the shipping industry has been a relatively safe zone for cybercrime over the past few decades due to the characteristics of ships separated from land networks. However, Cyberattacks on major global shipping companies such as COSCO and MSC have been taking place for four consecutive years since the NotPetya ransomware attack on Maersk in 2017 (Park, 2020). In addition, direct attacks on ships are increasing, with hackers taking control of a German container ship in 2017 and several Korean car carrier ships' computers being infected with ransomware in 2019 (Kim & Kim, 2019).

IMO adopted a resolution (MSC.428(98)) for the Maritime Cyber Risk Management in Safety Management System (SMS) in 2017 to respond to the rapidly changing cybersecurity environment in the maritime sector, which was implemented worldwide on 1 January 2021. Accordingly, the shipping companies shall establish cyber risk management measures in the company's SMS, and the flag states shall verify its adequacy in the company's SMS review, which is conducted for the first audit since 1 January 2021.

BIMCO, Intertanko, and Classification Societies, etc. have developed and provided Cyber risk management guidelines to support establishing the company's security management system. However, the contents of the guidelines are so vast and professional that it is difficult for ordinary shipping company employees to understand

and apply them to company's management system. In particular, small shipping companies that own one or two ships and do not receive consultation from external professional cybersecurity companies are more challenging to understand and apply the guidelines. In addition, it is necessary to understand the types and characteristics of various cyberattacks and to identify and reinforce the vulnerabilities of cyber risk management system of each company, but simply applying the security guidelines makes it difficult to improve vulnerabilities considering the characteristics of cyberattacks.

From this point of view, this paper will identify significant cybersecurity elements in the cybersecurity guidelines using previous studies and analyses the security vulnerabilities of shipping companies for identified individual items or cybersecurity fields. It also investigates the relationship between the company's characteristics (as the size of operation ships, cybersecurity personnel, etc.) between its cybersecurity vulnerabilities to determine what shipping companies should focus on most to improve their cybersecurity response capabilities.

1.2. Research Objectives

IMO and the global maritime industry recognized the importance of cybersecurity, and they introduced a cybersecurity risk management system from 1 January 2021. Several related organizations, including BIMCO, have developed cybersecurity management guidelines and provided shipping companies for managing security risks. However, so far, there has been no research on whether shipping companies in each country can implement the guidelines. The dissertation plans to sample Korean shipping companies and investigate their status of implementing the guidelines' security requirements and identifying cybersecurity vulnerabilities. Through this study, shipping companies will be expected to know the cybersecurity capabilities and cyber risk factors they need to focus on and strengthen. Understanding the measures to be focused is especially important for small shipping companies with limited resources.

1.3. Research Questions

In order to achieve the purpose of this paper, the study begins with the following two questions.

- Are Korean shipping companies implementing significant cybersecurity elements in cyber risk management guidelines provided by related organizations such as BIMCO?
- What is the correlation between the company's characteristics and its cybersecurity vulnerabilities?
- What strategies can IMO or States choose to improve cybersecurity vulnerabilities?

1.4. Scope of Study

The shipping industry is based on international interaction. A ship can sail to any port in any country in the world and exchange information with many stakeholders such as ports authorities, terminals, Vessel Traffic Services (VTS), and Shipping agents in the country. Therefore, it is reasonable that a global survey should be conducted to understand the cybersecurity status of the shipping industry. However, due to the limitations of time and information, it is challenging to investigate cybersecurity management situations in all countries of the world. Therefore, in this paper, Cases of a particular country have been sampled for the survey. The sampling country is South Korea. South Korea is one of the world's largest shipping countries. It has the advantage of reflecting on various shipping environments when investigating because both the coastal shipping industry and ocean-going shipping industry are developed. Above all, the ship management industry has developed. There is an association with 150 shipping companies as its members, making it relatively easy to obtain the necessary data through the association.

Cybersecurity research in the shipping industry can consider various targets such as ships, companies, transportation systems, and ports. An analysis of vulnerabilities can also be conducted among hardware such as computers and networks, software

such as vaccine programs, and cybersecurity management systems. However, this paper analyses how effectively shipping companies manage cybersecurity for their ships according to guidelines such as IMO and BIMCO. Therefore, the cybersecurity vulnerabilities of related organizations such as port authorities and the cybersecurity weaknesses of ship's computers or networks are excluded from the study in this paper.

1.5. Methods

Cybersecurity threat countermeasures that shipping companies must comply with will be identified by using previous studies and cybersecurity management guidelines from IMO and organizations such as BIMCO, International Electrotechnical Commission(IEC). The countermeasures are organized and listed in the term of cybersecurity elements. Cybersecurity elements are classified into three parts such as administrative security, technology security, and physical security.

An e-mail survey is conducted on Korean shipping companies and ship safety management companies for cybersecurity elements identified in the first stage. In addition, the survey examines the general status and the cybersecurity characteristics of companies together. The level of companies' implementation of cybersecurity elements is checked through questionnaire analysis.

Security vulnerability means the actual state of implementation of cybersecurity elements. The correlation between the security vulnerabilities identified in the previous step and the companies' characteristics, such as the company's size, maintaining security personnel, and utilizing external cybersecurity experts is analyzed.

The paper synthesizes the analysis results of the previous step, analyzes the strengths and weaknesses of Korean shipping companies in implementing cybersecurity elements, and suggests the most effective countermeasures to strengthen security vulnerabilities.

2. Literature review and Definitions

2.1. Literature review

Park et al. of Korea Maritime Institute [KMI] (2019) analyzed trends, security technologies, and cybersecurity policies of major countries through a Study on Strengthening Cyber-security System in the Maritime Sector and proposed measures to improve vulnerabilities in marine cybersecurity. In particular, 27 cybersecurity hazards were identified using BIMCO's security guidelines and ISO/IEC's security standards. In addition, in this study, risk assessment was conducted on the 27 identified cybersecurity elements, and based on the assessment, it was proposed to improve cybersecurity vulnerability. However, the risk assessment of cybersecurity elements is evaluated only by the possibility of occurrence and the magnitude of the impact, so it does not show how the shipping companies respond to each cybersecurity element.

Tam and Jones of the University of Plymouth (2018) performed a cyber-risk assessment on Autonomous ships by the MaCRA model. This work identified vulnerabilities in cutting-edge sensor networks and remote access, giving an exemplary insight into future automated ship security threats. Tam et al. (2016) also described various cyberattacks on ships in a study of threat and impact in Maritime cybersecurity based on scenarios. They suggested countermeasures against cyberattacks such as ship software updates and password usage. However, there is a limitation of model analysis with no empirical case investigation at all.

Jo Y.H. and Cha Y.K. of Korea University (2019) identified cybersecurity threats from ships in a study of cybersecurity requirements of ship Using Threat Modeling. The study evaluated the importance of each type of security threats through STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service) model, and identified possible threats for each element of the Data-flow diagram through analysis of various cyberattack cases, and proposed the separation of onboard networks to minimize cyber threats. However, it did not present an analysis of the ship

company's security management capabilities and a plan to strengthen the company's security accordingly

Androjna et al. (2020) analyzed the threats and incidents of various cyberattacks on ships, ports, and autonomous ships in an article titled Assessing Cyber Challenges of Maritime Navigation. In particular, this article evaluated the vulnerability of various equipment on ships such as GPS and eLoran through rich literature investigations as well as accident cases.

Song et al. (2018) analyzed the characteristics and types of recent cyberattacks and investigated cyberattack warning systems and analysis methodologies through a Korea Institute of Science and Technology report. In particular, this report is evaluated to give a better understanding of several cyberattack methods to the victim organizations and help to develop proper countermeasures against cyberattacks through in-depth analysis of actual attacks. However, this study has limitations in explaining the specificity of cybersecurity in maritime fields such as ship companies and ships.

Do (2019) investigated trends in international standards for cybersecurity and representative cybersecurity threat analysis techniques such as Microsoft's STRIDE model, Tony UcedaVelea's PASTA (The Process for Attack Simulation and Threat Analysis) model, SEI(Software Engineering Institute)’s OCTAVE(Operationally Critical Threat Asset and Vulnerability Evaluation), and ETSI(European Telecommunications Standards Institute)’s TVRA(Threat, Risk, Vulnerability Analysis).

Baltic and International Maritime Council [BIMCO] et al. (2020) developed the guidelines on cyber security onboard ships so that shipping companies can assess and manage cyber risks. The guideline provided guidance on overviews of cyberattacks, identification of cyber threats and vulnerabilities, risk assessment methods, protective measures, recovery plans, and incident investigations.

2.2. Definitions

This chapter defines the principal terms used in this paper. Since most terms have academic definitions, they will borrow definitions from other professional books or papers. However, some terms were coined to facilitate the description of this paper. There will be no need for an argument because the definition of terms made in this paper is only for the convenience of explaining the situation.

a) Coefficient of determination (R2): In statistics, the coefficient of determination R2 measures the model's ability to predict or explain results in linear regression settings. In general, a high R2 value indicates that the model is suitable for data (Enders, 2020). The value of R2 is obtained by squared Pearson correlation coefficient (R).

b) Company's cybersecurity capabilities: This results from measuring the environment in which the company can perform cybersecurity work on ships. Three areas of organization & human resources, employee expertise, education & training were investigated, and the results were analyzed in Chapter 6.1.4. (Author).

c) Cronbach's Alpha coefficient: This is a value that measures the internal consistency for the purpose of verifying the reliability of each measurement variable, and if it is 0.6 or higher, it is usually judged that the reliability is high reliable (Chae, as cited by Lee, 2012).

d) Cybersecurity: The activity or process, ability or capability to protect and/or defend information and communication systems and the information contained therein from damage, unauthorized use, modification, or abuse (Department of Homeland Security [DHS], as cited by Craigen at el.,2014).

e) Cybersecurity elements: Important measures to strengthen cybersecurity extracted from cybersecurity guidelines issued by organizations such as

BIMCO and ISO/IEC. In this paper, the list of security elements in Table 2 made by KMI is utilized (Author).

f) Cybersecurity managers: Employees in charge of cybersecurity of ships in a shipping company or ship management company (Author).

g) Cybersecurity manpower: The size of workforce held by a shipping company or a ship management company to perform cybersecurity work on a ship. A company's manpower is obtained by multiplying the company's number of cybersecurity managers by the average DR (Author).

h) Dedicated rate of cybersecurity manager (DR): It refers to the ratio of cybersecurity-related tasks of ships among the total tasks of cybersecurity managers (Author).

i) Interval scale: The interval scale is a type of metric scale and reflects quantitative values. In interval scales, the location parameters mode, median and mean can be calculated. An interval scale can always be divided into equal portion scales (Statista, 2021).

j) Likert scale: The Likert scale is an ordinal scale measuring subjective emotions and attitudes. However, when the Likert scale is used for many questions, the number of response cases increases rapidly, so it can be considered as an interval scale and analyzed by a parametric method (Kim et al., 2016).

k) Ordinal scale: Ordinal data is a categorical, statistical data type where the variables have natural, ordered categories, and the distances between the categories are not known. The ordinal scale is distinguished from the nominal scale by having a ranking. It also differs from the interval scale by not having category widths representing equal increments of the underlying attribute (Wikipedia, 2021).

l) Pearson correlation coefficient (R): This is a value obtained by dividing the covariance of two variables by the product of each standard deviation in data on an equal interval scale or proportional scale. It quantifies the linear correlation between the two variables X and Y. Pearson's correlation coefficient has a value between +1 and -1, +1 means a perfect positive linear correlation, 0 means no linear correlation, and -1 means a perfect negative linear correlation (Wikipedia, 2021).

m) Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences (DHS, 2010).

n) Risk assessment: product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making (DHS, 2010). Qualitative risk assessment is obtained by multiplying the Likelihood index and the severity index (Park et al., 2019)

o) Vulnerability: physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard (DHS, 2010). In this paper, the degree of implementation of the shipping company for cybersecurity elements is defined as vulnerability (Author).

3. Methodology

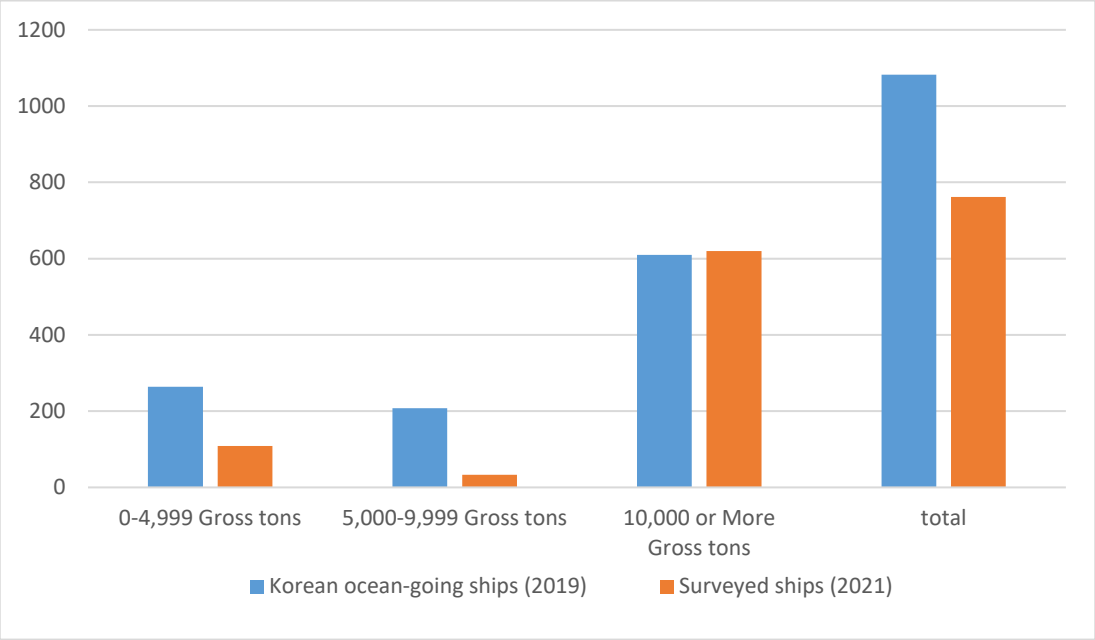
3.1. Data Collection

Data were collected by conducting a survey of South Korean shipping companies or ship management companies on their ship cybersecurity management status. The questionnaire in appendix 1 was used for the survey.

The questionnaire consisted of 46 questions in three areas. The first area is questions about the names, contacts, and companies of the people surveyed. The second area is a general field that consists of questions about general matters concerning ship cybersecurity management, including the size of the ship managed by the company, the number of ship security personnel, the implementation of security training, and the support of external experts. The third is questions about security elements to counter cyber threats, which are subdivided into administrative security, technical security, and physical security; each part has nine separate questions. The list of questions in this third area (a total of 27 questions in three parts) used a table on the cybersecurity risk factors of a study of Korea Maritime Institute (KMI), ‘A Study on Strengthening Cybersecurity System in Maritime Sector (2019)’. This table is made in consideration of the frequency of control failure and influence in the event of failure to control the ship's cybersecurity elements (Park et al., 2019).

The questionnaire was translated into Korean and distributed to about 150 Korean shipping companies and ship management companies to enhance the understanding of Korean participants. Of these, 38 valid survey results were collected from 22 companies (14.7% response rate). Some companies submitted several survey results, each written by a different person, and then the results were included in the statistical analysis in which the company’s redundancy was not problematic. Based on the number of companies, the survey response rate is very low at 14.7%. However, based on the number of ships, the response rate is high. This is because the number of management vessels of the companies that responded was 762 vessels, which is 70.4% of Korea's Ocean-going vessels as of 2019 (KMI, 2020).

Figure 1. Surveyed vessel status compared to the registered vessel (the surveyed vessel includes some domestic vessels)



The statistics are relatively less accurate because of differences at the time of surveys, and the 2021 surveyed vessels include some domestic vessels. However, referring to figure 1, it can be seen that almost all ships were surveyed for more than 10,000 gross tons (GT) of Ocean-going ships. On the other hand, only about 16 percent of ships between 5,000 GT and 9,999 GT were surveyed, while 41 percent were surveyed for ships less than 4,999 GT.

The IMO resolution on ship security (MSC 428) has been implemented, but most countries, including South Korea, have yet to enforce it. However, it is known that the US and Singapore are forcing the implementation of cyber security measures for ships and confirming them through PSC. In addition, oil carriers and bulk carriers have been implementing cybersecurity measures for ships since 2017 in accordance with the regulations of the Oil Major inspection and Bulk Ship Shipper Association. As a result, large ships that carry crude oil or bulk cargo and ships that sail to the US or Singapore are generally already implementing cybersecurity measures for ships before 2021. On the other hand, ships sailing only in South Korea's domestic ports and neighboring countries such as China, Japan, or Southeast Asia, are mostly not

implementing cybersecurity measures. This situation would explain figure 1, in which more than 10,000 GT of vessels have almost 100 percent response rate, while less than 10,000 GT have less than 50 percent response rate. More than 10,000 GT of ships are likely to be VLCCs or BULK Carriers, which carry crude oil or bulk cargo, and ships that sail to the USA or Singapore are bigger than ships that sail neighboring countries such as China, Japan, or Southeast Asia. Companies that manage ships sailing only in the nearby waters of Korea generally have low awareness of cybersecurity. In some cases, even the person in charge of cybersecurity is not designated, so they do not even take the survey questionnaires. On the other hand, as shown in the graph above, most companies that operate more than 10,000 GT of ships are believed to have filled out and replied to the survey questionnaires.

3.2. Data analysis

The company's cybersecurity management environment is identified through analysis of the first and second areas of the questionnaire. The analysis of the third area examines the security vulnerabilities of each company for each cybersecurity element. Eventually, it correlates the security vulnerabilities of each company with the characteristics of the company identified in the second area (management ship size, security manager number, security training, etc.).

3.2.1 Reliability analysis of data

Before analyzing the collected data, it is necessary to analyze the reliability of the data. Reliability analysis is an essential part of research methods that analyse how similar results are shown without being affected by time or circumstances, even if respondents repeat the same survey (Jeong & Choi, as cited by Lee, 2012).

This paper verifies reliability using the Cronbach's Alpha coefficient for 27 question answers in questionnaire area 3. Generally, a Cronbach's Alpha value of 0.6 or higher

is considered reliable, and 0.8 or higher is considered highly reliable (Chae, as cited by Lee, 2012).

Using the SPSS Ver. 28 program, the Cronbach's Alpha coefficient of questionnaire area 3 (27 questions) was calculated, showing very high reliability at 0.934. The Cronbach's Alpha values of three sub-parts of the questionnaire area 3 are respectively 0.878 (Sub-part 3-1 Administrative Security), 0.869 (Sub-part 3-2 Technical Security), and 0.825 (Sub-part 3-3 Physical Security), which also demonstrate high reliability. In other words, the survey results of the questionnaire area 3 to check the cybersecurity status of shipping companies mean that even if the environment or time of the survey is changed, it can produce quite consistent results.

Table 1. Reliability analysis result for the questionnaire Area 3 (Cronbach's Alpha)

	Administrative Security (9 questions)	Technical Security (9 questions)	Physical Security (9 questions)	Area 3 total (27 questions)
Reliability (Cronbach's Alpha)	0.878	0.869	0.825	0.934

3.2.2. Vulnerability Analysis

Wikipedia (2021) defines vulnerability as "a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege within a computer system." The Risk Lexicon of US Department of Home Land Security (DHS) (2010) defines as "characteristic of the design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation." However, unlike risk, vulnerability is not clearly defined to be measured in objective figures.

On the other hand, The risk can be expressed by multiplying the likelihood and severity in Equation (Yoo & Park., 2021). Therefore, it is easy to represent the degree of risk in objective figures. Yoo and Park (2021) conducted risk assessment on 27 cybersecurity elements (See table 2) through a survey of cybersecurity experts, which

obtained the value of risk levels for each security element as a multiplication of the frequency of accidents and severity of damage (See figure 2).

Table 2. cybersecurity elements (source: Journal of Marine Science and Engineering, 2021)

Security Areas	Risk Factors * in Case of Control Failure	Identification Code (ID)
Administrative Security	1. Raise awareness on information protection and conduct education targeting staff on board as well as on land	A1
	2. Access limitation of visitors (port-related officials, technicians, agents, etc.)	A2
	3. Upgrade hardware (H/W) and software (S/W), and S/W maintenance	A3
	4. Update anti-virus and malware prevention S/W tools	A4
	5. System of regulating remote access	A5
	6. Access to information is only allowed to authorized staff	A6
	7. Control the use of portable media (USB, portable PC, etc.)	A7
	8. Policy for discarding equipment including data	A8
	9. Establish contingency plans for cyberattacks	A9
Technical Security	1. Limitation and control of network port, protocol, and service	T1
	2. Configure network equipment such as firewall, router, and switch	T2
	3. Detect, block, and warn of cyberattacks through the system	T3
	4. Data encryption by utilizing a virtual private network (VPN)	T4
	5. Wireless access control with encrypted keys	T5
	6. Install anti-malicious code software and regularly install patch files	T6
	7. Hardware and software security configuration (system access limit excluding administrator)	T7
	8. Protect emails and web browsers	T8
	9. Support data backup and recovery	T9
Physical Security	1. Set up physical security area and access control	P1
	2. Design and apply physical security for office, working space, and facility	P2
	3. Access control and information system isolation of unauthorized users	P3
	4. Secure continuous availability and confidentiality from the cut-off of power supply and support facilities	P4
	5. Protect power supply and communication cables supporting data transmission and information facilities from being damaged	P5
	6. Ban on carrying any equipment, information, and software outside without prior approval	P6
	7. In case of reuse and discarding of equipment including storage media, remove data and licensed S/W and confirm the removal	P7
	8. Protect user information and check the management of unused equipment	P8
	9. Desk organization policy for documents and portable storage media	P9

Figure 2. The risk level of 27 cybersecurity elements (source: Journal of Marine Science and Engineering, 2021)

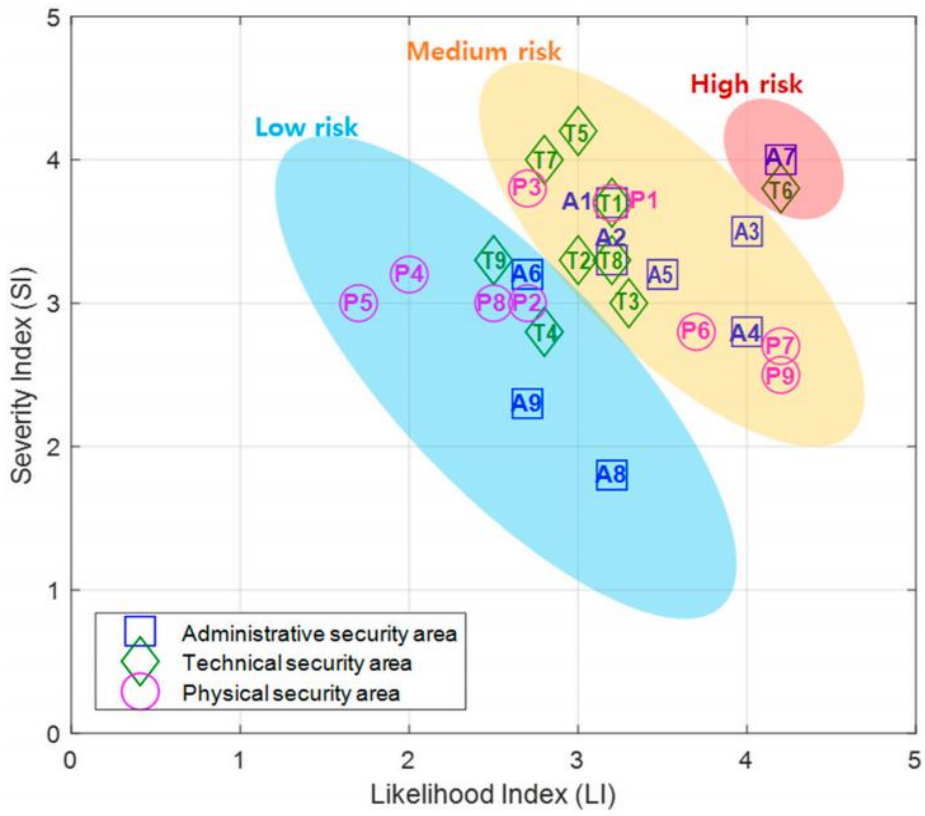


Figure 2 shows that A7[1](control the use of portable media) and T6[2](Install anti-malicious code software and regularly install patch files) are classified as high risks. Yoo and Park (2021) evaluated the confidence in the survey using the Analytic Hierarchy Process (AHP) and the Consistency Index (CI) to derive the above results. The high-risk levels of A7 and T6 may be empirically inferable, even if the adequacy of the method is not discussed. Portable equipment such as USB can always be an easy and effective striker in cybersecurity. In addition, computer systems that do not have anti-malicious code software or are not adequately patched can also be exposed

[1] A7 refers to Cybersecurity element No. 7 "Control the use of portable media(USB, portable PC, etc.)" of the Administrative Security part of Table 2.

[2] T6 refers to Cybersecurity element No. 6 "Install anti-malicious code software and regularly install patch files" of the Technical Security part of Table 2.

to cyberattacks at any time. Therefore, it may be natural that the A7 or T6 was analyzed as a high-risk element.

However, high-risk cybersecurity elements such as A7 and T6 do not always mean high vulnerabilities against cybersecurity threats. For example, mobile storage devices such as USB can be easily accessed and used by anyone, resulting in frequent cybersecurity incidents. Its large storage capacity can cause significant damage to the system. Therefore, No wonder mobile storage devices have a very high-risk value that is calculated by multiplying the severity and the frequency of the accident.

However, if a company prohibits using personal USB and uses USB authentication and security programs on all computers, the company's cybersecurity vulnerability to A7 items will be very low. That is, for 27 cybersecurity elements in Table 2, the level of cybersecurity risk and the cybersecurity vulnerabilities may not match.

In a Guide to risk and vulnerability analysis, the Swedish Civil Contingencies Agency (2012) stated that vulnerability analysis is to identify more detailed problems with scenarios in which risk analysis has already been performed. Therefore, in order to get a deeper understanding of cybersecurity, it is necessary to analyze vulnerabilities against 27 cybersecurity elements in Table 2 that Yoo and Park[3] (2021) or Park et al (2019) assessed for risk.

DHS Risk Lexicon (2010) defines a vulnerability as a possibility of success when an attack is attempted. Therefore, To identify vulnerabilities, it is more reasonable to evaluate how the victim is preparing for the attack, rather than assessing the possibility or magnitude of the attack's impact.

3 A study of Yoo and Park (2021), Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship, was published in English in the *Journal of Marine Science and Engineering* by extraction the risk assessment part from a Study on Strengthening Cybersecurity System in the Maritime Sector (Park et al., 2019).

The cybersecurity vulnerabilities of the companies surveyed are identified using a Likert 5 points scale (See Table 3) for 27 cybersecurity elements of Table 2. Kim et al. (2016) said that the Likert scale is categorized as an ordinal scale because it measures individual subjective emotions and attitudes. Therefore it is generally inappropriate to use parametric methods for the Likert scale. However, Kim et al (2016) also said that if the Likert scale is used for many questions, the number of possible response cases increases rapidly, so it can be considered as interval scale and thus analysed as parametric method. Therefore, 27 questions in Area 3 (Ship Cybersecurity Management) of Appendix 1 used the Likert scale can be analysed using the parametric method. However, the average value for individual questions is not statistical values for many questions. So it just will use to check trends rather than statistical meanings.

As you can see in Table 3, The respondents were asked to select (1) 'Strongly disagree' if they considered the most vulnerable to the question item and (5) 'Strongly agree' if vice versa. Therefore, the most vulnerable element of cybersecurity gets one point, and the least vulnerable element of cybersecurity gets five points. In addition, 'Not applicable' can be selected if the answer to the question is not understood, considering the respondents who are not familiar with cybersecurity tasks. 'Not applicable' was excluded from vulnerability analysis for selected items. This is to increase the reliability of the survey by preventing a rough guess from responding without an understanding of the exact cybersecurity status of their own company or vessels.

Table 3. Likert 5 points scale of answers for Appendix 1 Area 3 questions

Point	(1)	(2)	(3)	(4)	(5)	(0)
Status	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable

The vulnerability of individual companies was determined by the average of the answers to 27 items in Area3 of the questionnaire. The smaller the average value means the greater the vulnerability to cybersecurity, and the evaluation of the degree of vulnerability is based on Table 4. The quantifiable evaluation of survey results, such

as Table 4, is because the statistical processing results of many Likert scale questions can be considered interval scale, not ordinal scale.

Table 4. Vulnerability Rating table

Average value	1.0 ~ Less than 1.8	1.8 ~ Less than 2.6	2.6 ~ Less than 3.4	3.4 ~ Less than 4.2	4.2 ~ 5
Vulner-ability Rating	Very Vulnerable	Vulnerable	Neutral	Invulnerable	Very Invulnerable

3.2.3. Correlation Analysis

The level of cybersecurity vulnerabilities in individual companies can be identified through questionnaire analysis. However, vulnerability analysis does not show why each company represents such a difference in cybersecurity level. In this paper, the correlation between company characteristics (such as the size of the company, cybersecurity personnel, education and training) and security vulnerabilities is found through correlation analysis.

Correlation analysis can use parametric and nonparametric methods depending on whether the data are normally distributed. Parametric methods include Pearson correlation, and nonparametric correlation involves Spearman and Kendall's Tau. However, we confirmed earlier that even the original ordinal scale could be considered an interval scale if the number of questions increases. Therefore, parametric methods can be used for Likert scale surveys with multiple questions. In the end, one of the parametric methods, Pearson correlation analysis, can be used to correlate the value of a company's security vulnerability derived from the result of the Likert scale survey of multiple questions.

Correlation is analyzed between the company’s characters such as the number of management vessels, total tonnage of ships, cybersecurity personnel, expertise in cybersecurity managers, education & training and the company's cybersecurity

vulnerabilities using an Excel program's Pearson correlation tool(the Scatterplot Trend Line and CORREL function).
Correlation refers to the relevance of changes in two variables, and covariance can mathematically explain the relevance. Pearson correlation coefficient(R) adjusted the range of covariances from -1 to +1 to facilitate the interpretation of correlations.

A value of r of 0 indicates that there is no linear relationship between the two variables, and a larger absolute value of r means that the relationship between variables becomes stronger, and an absolute value of r of 1 means that all data is precisely in a straight line (Patrick et al., 2018). Several methods are proposed for the interpretation of correlation coefficients, and Table 5 is one of the examples.

Table 5. Example of a Conventional Approach to Interpreting a Correlation Coefficient (Source: Patrick et al., 2018)

Absolute Magnitude of the Observed Correlation Coefficient	Interpretation
0.00-0.10	Negligible correlation
0.10-0.39	Weak correlation
0.40-0.69	Moderate correlation
0.70-0.89	Strong correlation
0.90-1.00	Very strong correlation

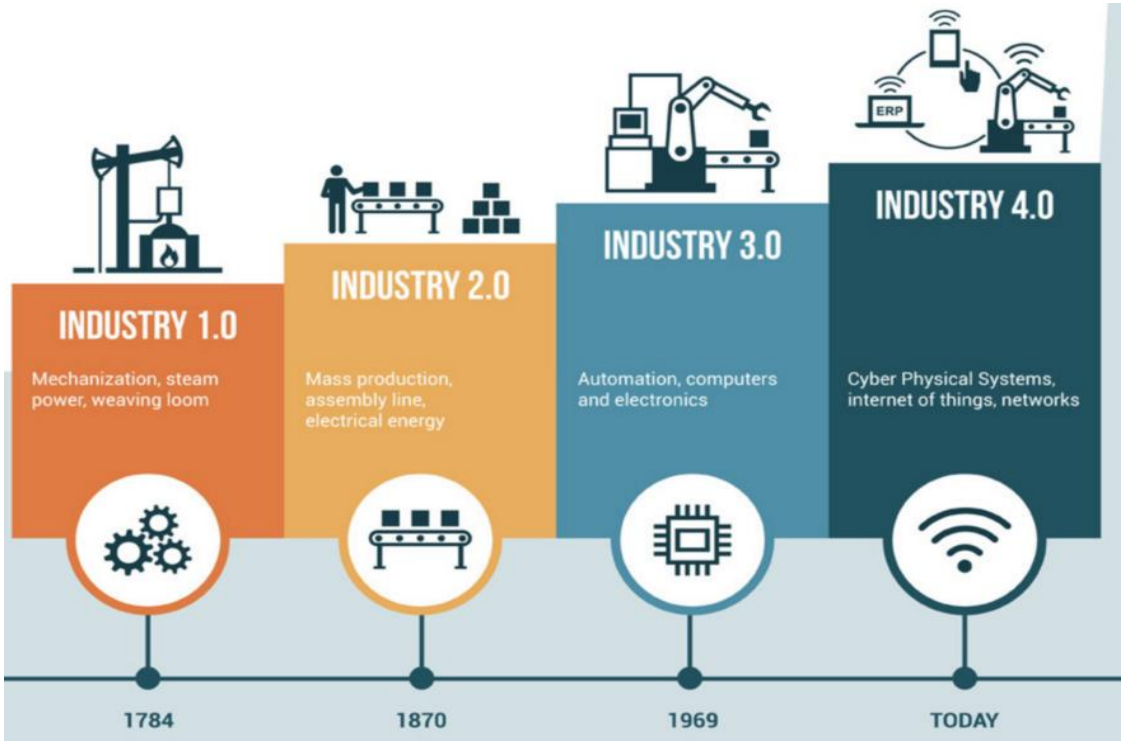
Patrick et al. (2018) noted that in interpreting correlation coefficients, it is desirable to interpret the relationship strength of a particular coefficient in the context of scientific questions rather than mechanically applying the analysis criteria, as shown in the example above. Therefore, it is desirable to understand that although this paper also basically correlates with the criteria in Table 5, it merely represents the tendency of relationship strength between variables.

The coefficient of determination is calculated in addition to the correlation coefficient analysis. The coefficient of determination(R^2) can be obtained by the square of the r value, indicating the degree to which the estimated linear model fits the given data.

4. Overview of Cybersecurity

The fourth industrial revolution, which has terms such as big data, cloud computing, artificial intelligence, and cyber-physical systems as its core concepts, is now having a massive impact on our world. Suppose the third industrial revolution is the transition from analogue to digital. In that case, the fourth industrial revolution is characterized by the combination of industry, automation, digitalization, and Internet of Things (IoT) technologies (Adebayo et al., 2019).

Figure 3. The four levels of the Industrial Revolution (Source: JMESS, 2019)

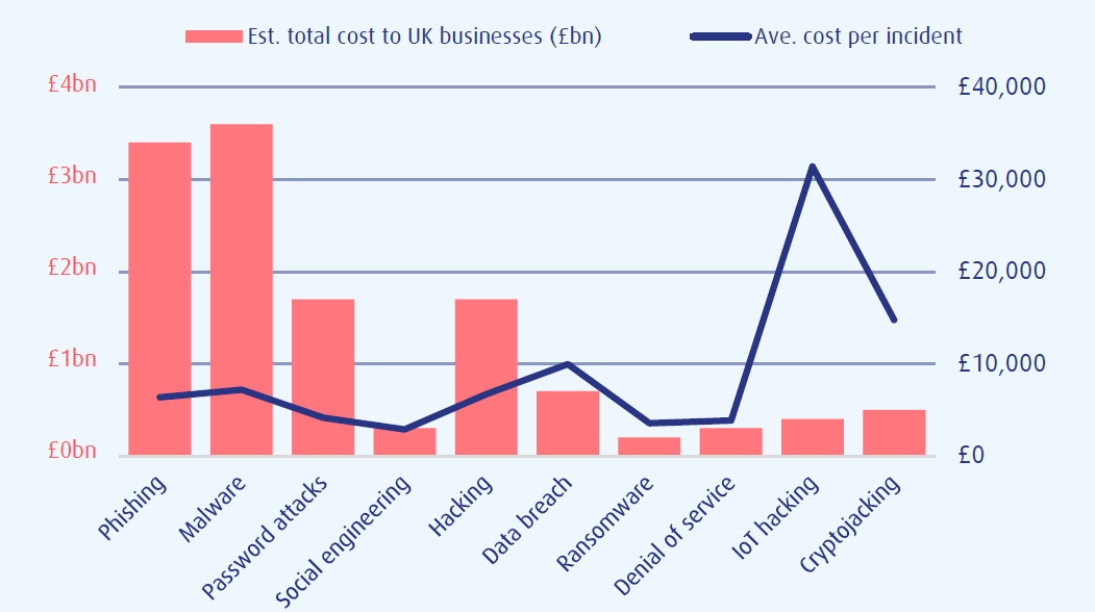


In particular, the 4th industrial revolution is accelerating further as the commercialization of 5th generation mobile communication(5G), a core infrastructure of the 4th industrial revolution, is promoted worldwide. 5G's data communication speed is about 40 times faster than the 4th generation(4G) Long Term Evolution (LTE) mobile communication technology. It can connect 1 million IoT devices within 1km at the same time and has a communication delay of 0.001 seconds or less, which is

expected to play an important role in IoT, autonomous driving, Virtual/Augmented Reality (VR/AR), Cloud computing, Big Data, Artificial intelligence (AI) (Kim & Lee, 2018).

Although there is no doubt that the 5G network will play an essential role as a spinal network of the 4th industrial revolution due to the characteristics of high-speed large-capacity communication, high-reliability ultra-low-latency communication, and mass-connected communication, Cybersecurity risks are expected to increase exponentially due to complex connections between 5G network and existing communication networks (4G,3G), the Internet, and various IoT devices. In particular, deterioration in security performance caused by differences in security characteristics between other devices or networks connected to 5G networks can be a big challenge (Kim et al., 2019).

Figure 4. the business cost of cybercrime incidents in 2019 (Source: Beaming)



According to Five Years in Cyber Security (2020) of Beaming, British companies lost nearly £13 billion in 2019 due to cybercrimes such as phishing, malware, ransomware, and hacking. The average loss per crime is about £6,000, with IoT hacking the largest

loss per case at about £31,000, followed by Cryptojacking at about £150,000. The type of cybercrime that caused the greatest loss is phishing, and the type of crime that caused the smallest damage is ransomware (See Figure 4). Here, we looked at cases of cybercrime damage in a country like the UK, but most countries where informatization is developed in the world are exposed to such various forms of cybercrime, and the damage is increasing every year. In a special report on cybersecurity, Morgan (2020) predicted that global cybercrime-related costs, which stood at $6 trillion in 2021, will increase by 15% annually to $10.5 trillion by 2025.

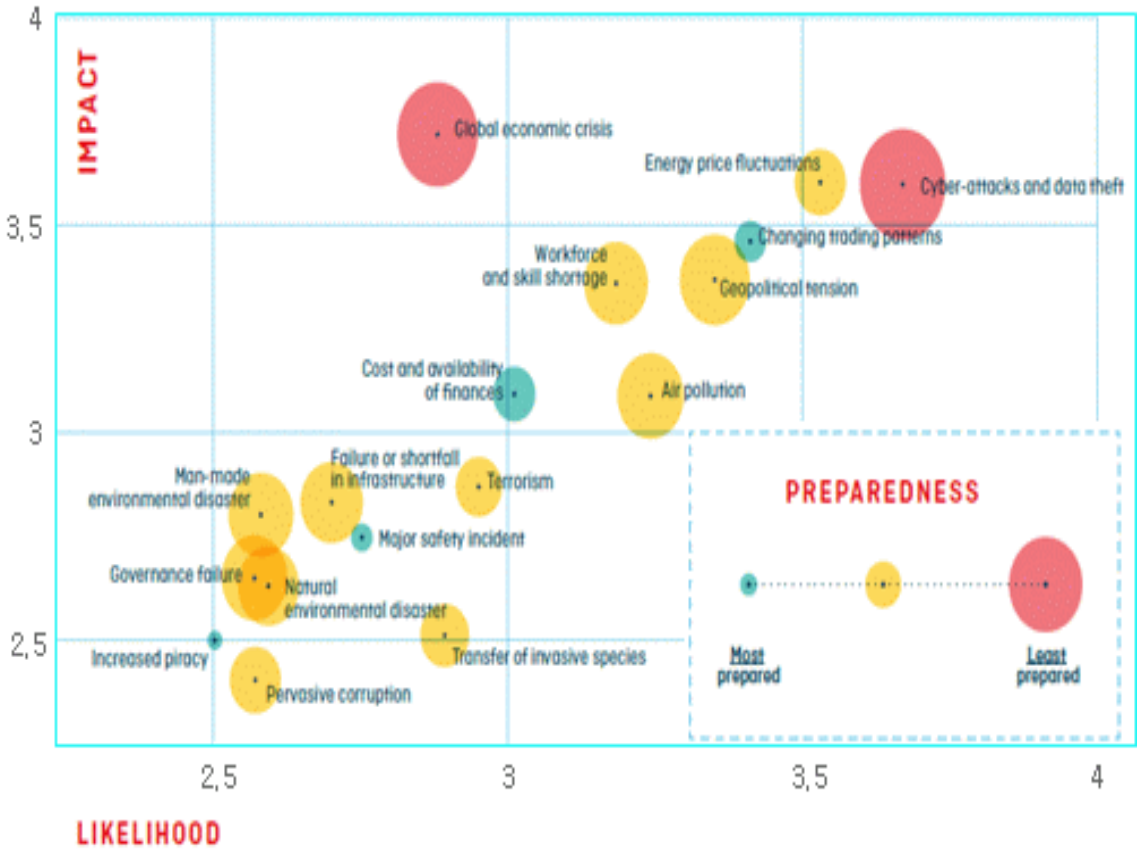
The reason why cybercrime is increasing is that it has become easier to commit cybercrime with the use of new technologies such as the automatic creation of malware and the development of the stolen data black market. And revitalization of the virtual currency market has made it easier to cash in cybercrime (Ha, 2019). As time goes by, the cybersecurity environment is expected to become more complex because the spread of 5G networks and IoT devices can be a means for cybercriminals to access targets at high speed through various channels.

To cope with this situation, the international community and countries around the world are preparing countermeasures against cybercrime. First of all, the International Telecommunication Unit (ITU) created guidelines for establishing cybersecurity policies in each country in 2011. The United States enacted and implemented the E-Government Act in 2002 for information security and confidential information protection. In 2014, Federal Information Security Modernization Act, National Cybersecurity Protection Act, and National Cybersecurity and Critical Infrastructure Protection Act were enacted or revised to protect vital infrastructure. In the case of Japan, the National Center of Incident readiness and Strategy for Cyber Security (NISC) was established and operated as a state agency under the Basic Act on Cyber Security in 2015. In Korea, the Information and Communication Infrastructure Protection Act was enacted and implemented in 2001 to protect information and communication-related infrastructure. In 2019, the Information and Communication Network Act was revised to protect the information in the private sector.

5. Cyber threats in the maritime sector

Stokes et al. (2018) investigated the perceptions of senior maritime stakeholders from more than 50 countries and reported that "cyber attacks and data theft" will become the most critical issue in maritime trade over the next decade. In particular, it was analyzed that cyberattacks and data theft issues are most likely to occur among major issues, and their impact is very large. On the other hand, the maritime industry's readiness for this issue was found to be the weakest.

Figure 5. Global Maritime Issue map (Source: Global Maritime Forum (2018), Global Maritime Issue Monitor 2018, p7)



In fact, cyberattacks in the maritime industry seem to have been increasing recently. Cyber-attacks on large shipping companies such as MSC have been occurring for the fourth consecutive year since 2017, and Safety4sea (2020) said important cyber-

attacks on operational technology (OT) in the maritime industry had increased nearly ten times from 50 cases in 2017 to almost 500 cases in 2020.

However, as shown in Table 6, shipping companies and ports still occupy most of the cyberattacks in the maritime sector rather than ships.

Table 6. cases of cyberattacks in the maritime sector

Attacked Date	Target	Attack Methods	outcome	Response	Source
2017.2	8,250 TEU German-owned container ship	Take control of Ship's OT system	Hackers took full control of the navigation system of the ship for 10 hours	The ship had to bring IT experts on board to regain control	Fairplay & Safety at Sea(SAS)
2017.6	Maersk line's digital infrastructure	Not Petya virus (ransomware)	$250-300 Million financial loss	Re-Installed 45,000 PCs, 2,500 applications	Digital Ship
2017.11	Clarksons's computer system	Single & Isolated user account (Unauthorised access)	Unauthorized access to the company's computer system	Clarksons took Immediate steps to respond to the incident	Digital Ship
2018.7	COSCO's Long Beach customer service center	Cyberhackers (ransomware)	COSCO's website and toll-free number were down	unknown	Professional Mariner

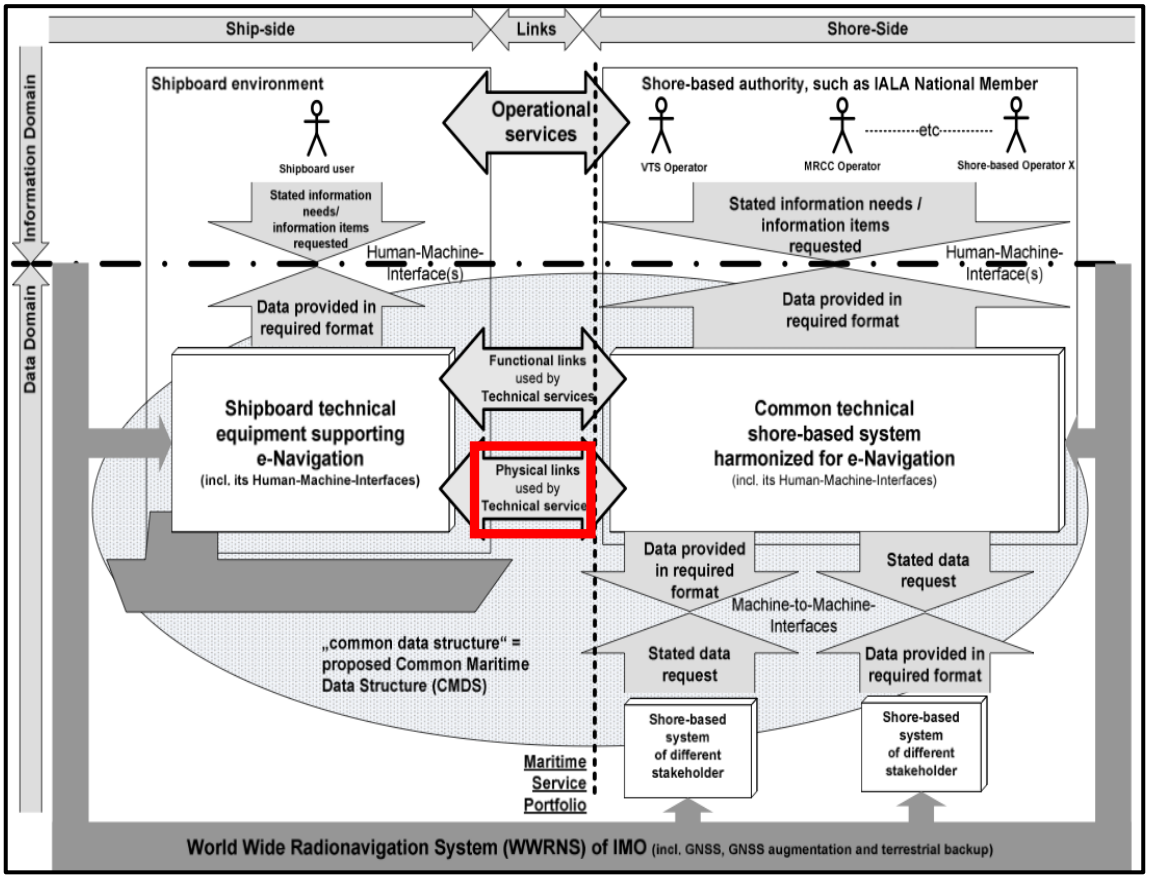
2018.7	COSCO US branch's business system	Ransomware attacks on e-mail systems and networks	Discontinued COSCO business e-mail and telephone service in the US Regions	System recovery	KMI
2018.9	Port of San Diego	Hackers who were demanding Bitcoins (ransomware)	Ransomware had penetrated its system	Shut down computers of port operation	Seatrade Cruise News
2019.3	'H' shipping company Car carriers	Ships' main computers Infection with ransomware by the e-mail file impersonating the Police Agency.	Become unusable of ships' computers	Infection computer format, loss data rewritten again.	FINANCIAL NEWS
2020.4	MSC's Data-center	Data-center attacked by malware	Main customer websites were down for several days	Customer Website restoration	Seatrade Maritime News
2020.9	US Tug boat	Spoofing attack through an attached file of voice e-mail	None	Report it to the relevant authorities	Ship-technology.com
2020.9	CMA CGM Container transportation main system	Online system ransomware (Ragnar Locker) attack	Container transportation reservation and transportation confirmation system down.	Services (booking, tracking, invoice, etc.) be restored in 2 weeks.	Shipping NewsNet

In line with the recent trend of technological innovation on land, various technological innovations such as e-Navigation, autonomous ships are accelerating in the shipping

industry. The application of advanced ICT technology to ships means that there will be a channel of connection between ships and land networks. Eventually, as discussed in the previous chapter, the threat in terms of the cybersecurity of ships will increase as the ship's computer (or system) access increases.

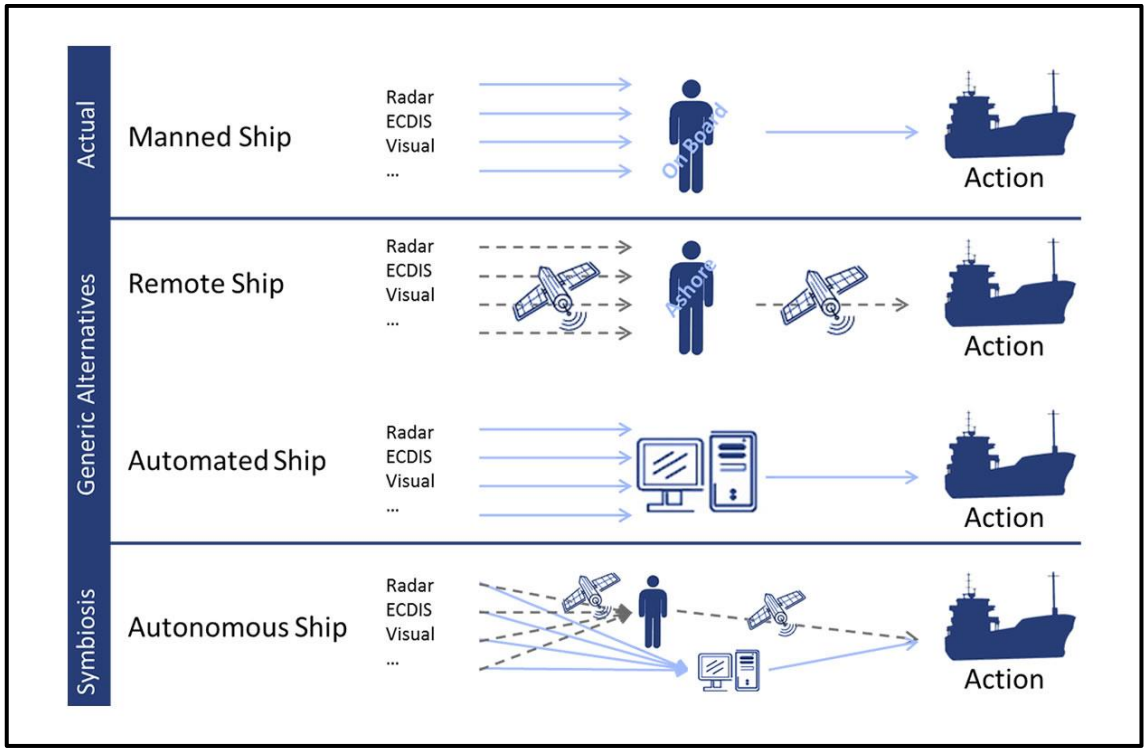
As can be seen from the IMO e-Navigation architecture in Figure 6 below, physical connections between land systems and ship systems must exist for various e-navigation services.

Figure 6. IMO overarching e-navigation architecture (Source : IMO)



In addition, the Autonomous Ship concept of MUNIN (Maritime Unmanned Navigation through Intelligence in Networks) Project also explains that communication between the systems of these ships and the land system is necessary to control the Autonomous Ship or Remote Ship (See Figure 7).

Figure 7. The Autonomous Ship concept of MUNIN (Source: MUNIN)



IMO adopted a resolution to integrate the guidelines for cybersecurity into ships SMS in 2017, taking into account the ever-increasing trend of cyberattacks and advanced ICT technology application to ships in the maritime industry. The resolution has been in effect since January 2021. In addition, BIMCO has produced and distributed cybersecurity guidelines for the cybersecurity work of ship companies.

However, unlike land's responses to enacting and implementing cybersecurity-related laws or establishing government organizations responding to cyberattacks, even IMO's resolutions are not mandatory but recommendations. Due to the nature of ships sailing around the world, it isn't easy to establish a land-level cybersecurity system for the maritime industry with a country's efforts. Therefore, first of all, cybersecurity guidelines provided by IMO or BIMCO should be faithfully implemented by shipping companies around the world, and cybersecurity should be sufficiently considered when designing the architecture of e-Navigation or autonomous ships.

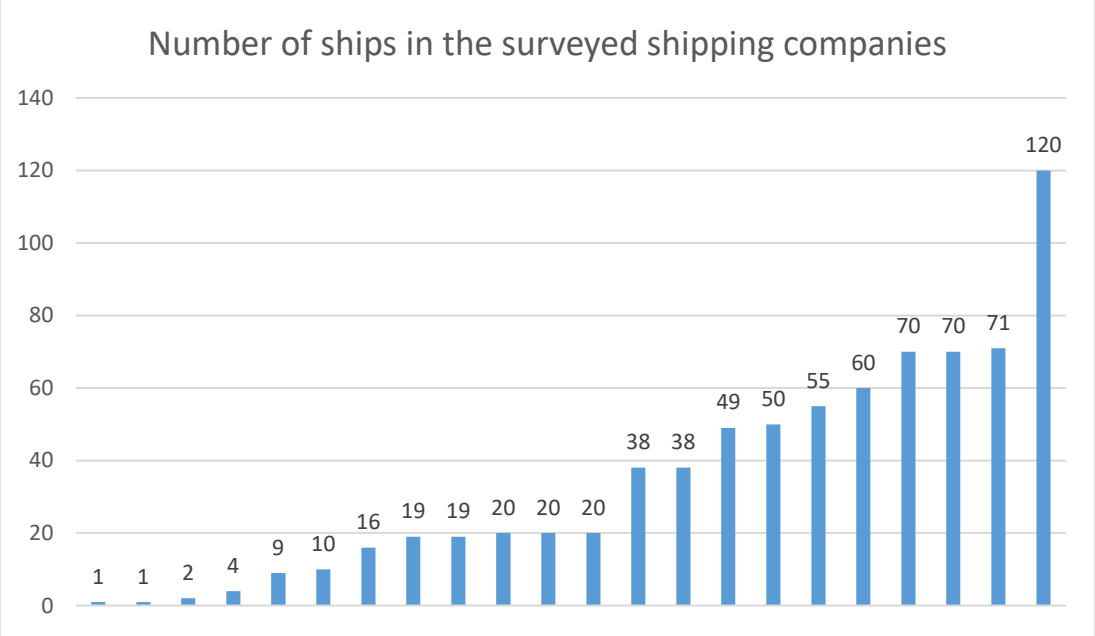
6. Analysis of Vulnerability of Korean shipping companies on Cybersecurity Threats

6.1. General status

6.1.1. Size of managed vessels of the surveyed companies

The survey of Appedix1 questionnaire received a total of 38 responses from 22 companies. The number of management vessels of these companies varied from at least one to up to 120, but almost all companies have more than ten vessels except for five companies. The total number of ships managed by the companies was 762, and the average worked ships for one company was 34.6.

Figure 8. Distribution of managed ships in surveyed companies



According to the size distribution of the ships managed by these companies, the ship's number of 10,000 GT or more is 620, accounting for 81.4 percent of the total, and the ship's number of less than 10,000 GT is 142 accounting for 18.6 percent. Among the 22 companies, eight were identified as having an average ship's size of less than 10,000 GT, and 14 companies were identified as having an average ship's size of 10,000 GT or more. In addition, companies that manage more than 10,000 GT of vessels have high response rates on questionnaires, which was explained in Chapter 3.1.

6.1.2. Establishment of cybersecurity management procedures

Of the 38 respondents, 31 were aware that the IMO resolution on the Maritime Cyber Risk Management in Safety Management System (MSC. 428) was implemented in January 2021, and only seven respondents were unaware.

In addition, 26 out of 38 respondents said that the company's SMS had incorporated regulations on cybersecurity under MSC.428, three responding to "NO" and nine responding to "Unknown."

33 out of 38 respondents said the procedure of cybersecurity management was established, two did not, and three did not know whether the company established its own cybersecurity procedures regardless of the integration of cybersecurity regulations to ship's Safety Management System.

When asked why the cybersecurity management procedure on ships was established, there were 20 cases respectively of cybercrime prevention and IMO's recommendations for ships, followed by 11 PSC responses and seven shippers' demands. This question can be answered multiple times, so the number of responses was higher than the total number of responses.

6.1.3. Cybersecurity manpower in the company

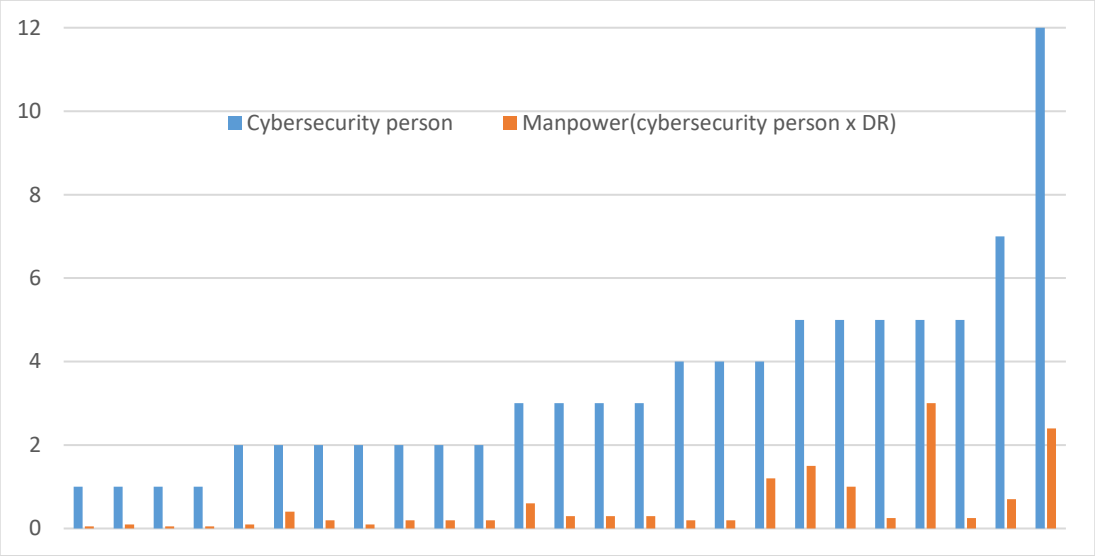
In a survey of the company's cybersecurity managers, four companies have no cybersecurity manager, five companies have one manager, nine companies have two managers, five companies have three managers, five companies have four managers, seven companies have five managers, one company has seven managers, and one company has 12 managers.

And the company's cybersecurity manager was asked how much of an individual's work time is related to cybersecurity. Regarding this question, One company answered 60%, two companies were 30%, four companies were 20%, nine companies were 10%, eight companies were 5%, and the rest did not answer. Here, these rates are called the dedicated rate (DR) of cybersecurity managers.

DR is an important factor in determining the size of the company's actual cybersecurity workforce. For example, a company with five cybersecurity managers with 20% DR has the same manpower effect as a company with one cybersecurity manager with 100% DR.

The following graph shows the results of calculating the Manpower of the company's ship cybersecurity work with the surveyed value of DR. The blue bar represents the number of ship cybersecurity managers by company. Orange bars represent Manpower for ship cybersecurity work as a result of multiplying the number of security personnel by the DR. In the graph, the number of cybersecurity managers varies from 1 to 12, and the average number of cybersecurity managers in 25 companies is 3.44 people. Manpower has a minimum of 0.1 to a maximum of 3 and an average of 0.554. Here, one manpower means that one cybersecurity manager performs 8 hours of cybersecurity-related work on one working day. The graph below shows that most companies have more than one cybersecurity manager on the surface, but in reality, most companies operate cybersecurity personnel with less than one.

Figure 9. Manpower of cybersecurity managers



6.1.4. Company's cybersecurity capabilities

Parts 2-8 through 2-9 of Appendix 1 assess the company's capabilities in terms of ship cybersecurity. The question is whether the company has sufficient organizational and human resources for managing ship cybersecurity, whether the company's cybersecurity managers have sufficient expertise, and whether the company provides adequate education and training about ship cybersecurity. For each survey, 5-point Likert scale was used as same as Table 3.

Table 7. Company's cybersecurity capabilities

	Very Vulnerable (1~1.8)	Vulnerable (1.8~2.6)	Neutral (2.6~3.4)	Invulnerable (3.4~4.2)	Very Invulnerable (4.2~5)
organizational & human resources		▪ 2.57			
expertise			▪ 2.94		
Education & training			▪ 2.82		
total			▪ 2.69		

The survey results showed that the vulnerability of the company's comprehensive ship cybersecurity response capability was Neutral at 2.69. However, the organizational & human resources sector is 2.57 points, showing the rating of Vulnerable. On the other hand, the expertise, education & training sectors had 2.94 and 2.82 points, respectively, indicating the rating of Neutral.

The company's cybersecurity capability were analyzed for companies with an average ship's size of less than 10,000 GT and companies with an average ship's size of 10,000 GT or more.

Companies with an average ship's size of less than 10,000 have weak security capabilities for all items. In particular, the organizational & human resources sectors were found to be the most vulnerable among the three items with 1.9 points, and when the three items were evaluated comprehensively, they were more vulnerable with 1.87 points.

Table 8. Cybersecurity capabilities of companies with an average ship's size of less than 10,000 GT

	Very Vulnerable (1~1.8)	Vulnerable (1.8~2.6)	Neutral (2.6~3.4)	Invulnerable (3.4~4.2)	Very Invulnerable (4.2~5)
organizational and human resources		▪ 1.9			
expertise		▪ 2.14			
Education and training		▪ 2.0			
total		▪ 1.87			

For companies with an average ship's size of 10,000 GT or more, the organizational & human resources sectors of the company's cybersecurity capabilities were found to be weak, but the rest were all normal.

Table 9. Cybersecurity capabilities of companies with an average ship's size of 10,000 GT or more

	Very Vulnerable (1~1.8)	Vulnerable (1.8~2.6)	Neutral (2.6~3.4)	Invulnerable (3.4~4.2)	Very Invulnerable (4.2~5)
organizational and human resources		▪ 2.57			
expertise			▪ 2.94		
Education and training			▪ 2.82		
total			▪ 2.69		

Although the results above do not use scientific analysis methods such as correlation analysis, it can be inferred that the size of the management vessel is related to the company's cybersecurity response capabilities, as the tendency of the two cases is evident. In the next chapter, this inference is verified through this correlation analysis method.

Cybersecurity managers responded to the question of what is needed to strengthen the company's ability to respond to cybersecurity as follows: Securing professional personnel and strengthening education & training accounted for the largest portion of the answers with 18 cases. The operational guidelines for cybersecurity tasks is 7 cases, 6 cases are about providing vaccine programs and security facilities, and 2 cases are about new dedicated organizations or the attention of the chief executive.

6.1.5. Support from outside experts

Five out of 22 companies have been confirmed to be supported by outside experts (or companies) to respond to cybersecurity tasks for ships. The company's cybersecurity managers said they were generally satisfied with the cybersecurity response capabilities of outside experts. Although a company rated dissatisfaction,

the average satisfaction score was 3.4 points out of 5 points. This is significantly higher than the company's evaluation score of 2.69 points for its own cybersecurity response capabilities.

It has been confirmed that the company's cybersecurity managers hope to expand the use of external experts, including direct and integrated management support rather than remote management, increase the scope of the professional workforce and related budget.

6.2. Vulnerability Analysis

6.2.1. Comprehensive analysis

Appendix 1 was used to investigate the company's cybersecurity vulnerabilities. Cybersecurity elements consist of a total of three parts: Administrative Security (AS), Technical Security (TS), and Physical Security (PS). AS assesses the state of the company's policies and support for cybersecurity response, and TS assesses technical access controls and measures such as encryption of ships' computers and networks. And the last PS assesses the vessel's physical management status, such as marking and locking for non-approved access control of the security zone.

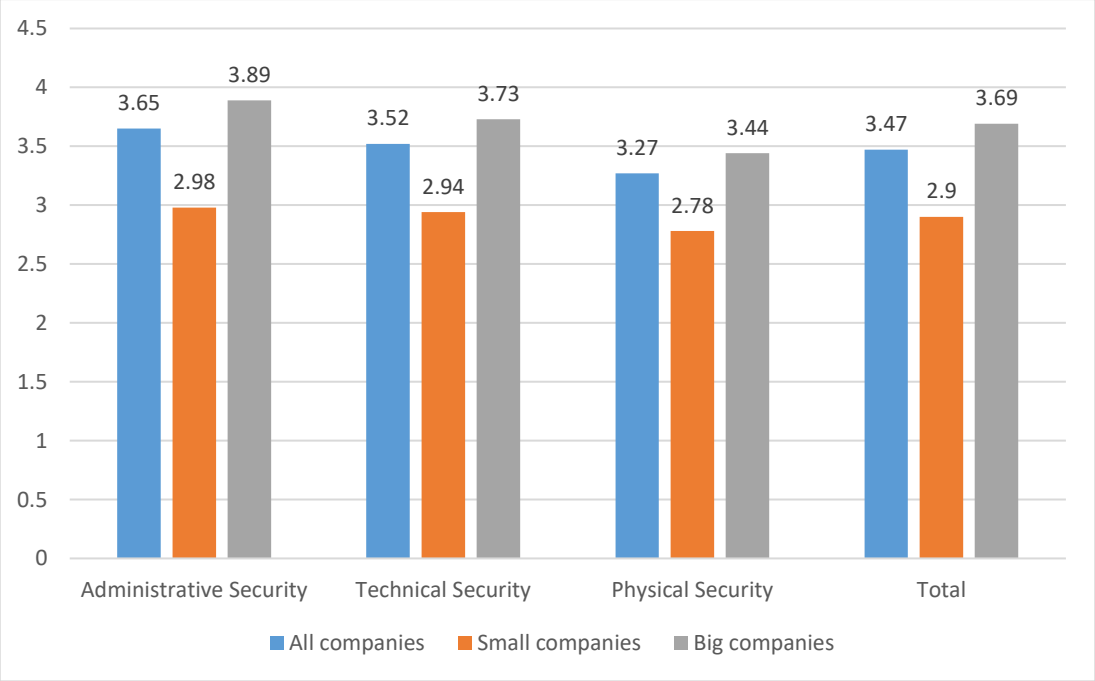
According to the vulnerability analysis, the overall vulnerability was found to be relatively good at 3.47 points. The vulnerability of AS was 3.65 points, The vulnerability of TS was 3.52, higher than the overall score, and the vulnerability of PS was 3.27, which is slightly lower than the overall score.

According to a cybersecurity vulnerability analysis by the size of the company, companies with an average ship’s size of less than 10,000 GT had overall scores of 2.9 points, and administrative, technical, and physical security fields are 2.98, 2.94, and 2.78 points, respectively. It had a lower value for all parts compared to the vulnerability value for the entire company. In particular, there was a bigger difference

in all areas compared to large shipping companies with an average ship's size of 10,000 GT or more.

Despite the company's size classification, the Physical Security part had the lowest score among the three security parts. This can be estimated that there are not many physical measures yet to be taken to strengthen the cybersecurity on individual vessels, and the details are to be analyzed in the Physical Security sector below.

Figure 10. Cybersecurity Vulnerability of Korean Shipping Companies (Overall)



Regardless of the companies' average scores, there is a big difference between the lowest overall scored company(1.74 points) and the highest overall scored company(4.88points). The company with the lowest score was managing 19 vessels (vessels between 100 and 5,000 GT) without a dedicated staff in charge of ship cybersecurity, and it was found that the company did not conduct any special training or education about ship cybersecurity. The highest-scoring company, on the other hand, had four employees in charge of cybersecurity on 38 large ships with more than 10,000 GT, and the employees were highly satisfied with the company's expertise, education and training.

The distribution of cybersecurity vulnerability scores by the type of companies in the table below shows that the overall vulnerability is relatively good as 22 companies are gathered in the Invulnerable and Very Invulnerable area. However, for small companies with smaller average sizes of vessels, the vulnerability scores are mostly distributed in subnormal areas compared to the Big Company group with larger average sizes of vessels.

Table 10. Cybersecurity Vulnerability Score Distribution

Vulnerability rating	Very Vulnerable (1.0~Less than 1.8)	Vulnerable (1.8~Less than 2.6)	Neutral (2.6~Less than 3.4)	Invulnerable (3.4~Less than 4.2)	Very Invulnerable (4.2~5)
Big companies	1	0	7	13	6
Small companies	1	3	3	3	
Total	2	3	10	16	6

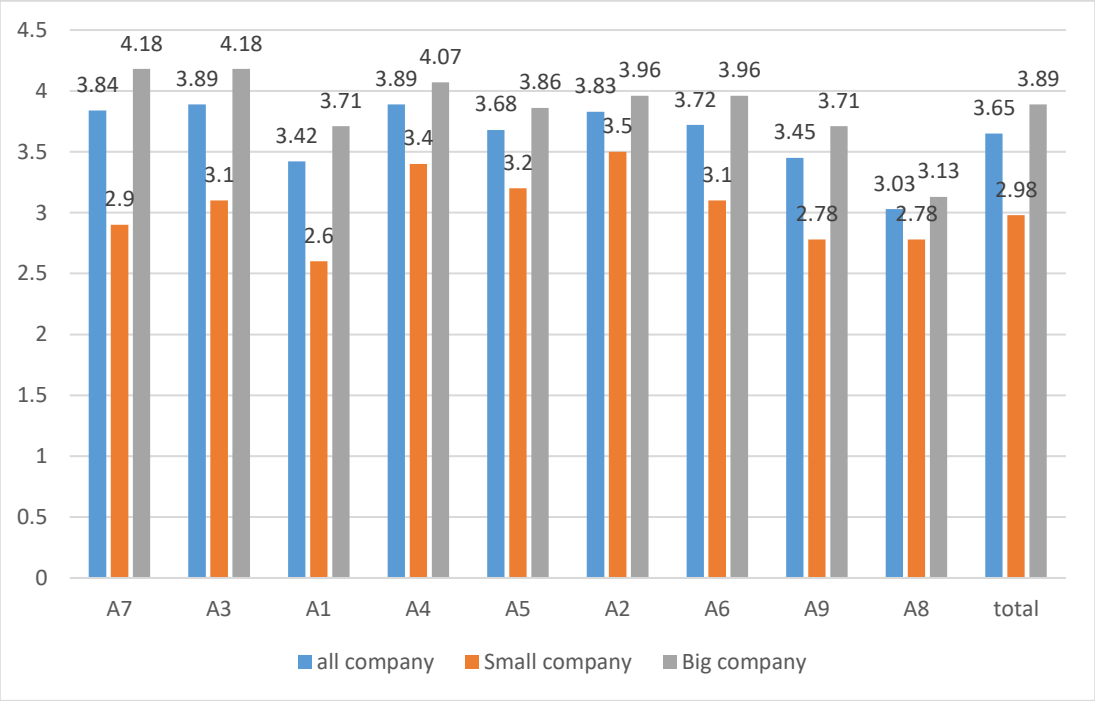
6.2.2. Administrative Security Analysis

The evaluation items of the Administrative Security part are as shown in Table 11, which uses data on the KMI prior Study on Cybersecurity, as mentioned earlier. The identification code for Table 11 also comes from Table 2. The order of the Cyberseruity elements on Table 11 was made in order of the larger risk of the Cybersecurity elements in the KMI prior study. That is, 3-1-1 element has the highest risk (Likelihood x Severity), and 3-1-9 element has the lowest risk.

Table 11. Administrative Security items & Identification code

Cybersecurity elements	Identification Code
3-1-1. There is control over the mobile media (USB, mobile PCs, etc.) used in ships.	A7
3-1-2. Periodic upgrades and ongoing maintenance of H/W and S/W of ship computers* are performed.	A3
3-1-3. Trainings for ship and land staff are provided periodically to raise awareness on information protection.	A1
3-1-4. Anti-virus and anti-malware S/W tools supplied for ship computers.	A4
3-1-5. The policy of controlling remote access to ship computers is being implemented.	A5
3-1-6. Restricting access to ships (port officials, technicians, agents, etc) is being implemented.	A2
3-1-7. Access to sensitive information is granted only to authorized employees.	A6
3-1-8. Emergency plans are in place for cyberattacks.	A9
3-1-9. Equipment disposal policies, including data, are being implemented.	A8

Figure 11. Cybersecurity Vulnerability of Korean Shipping Companies (AS Part)



The Administrative Security part has been shown to have a better security vulnerability than the other two parts (Technical and Physical). In particular, A7 (3.84 points), A3 (3.89 points), A4 (3.89 points), and A2 (3.83 points) elements get a relatively high score.

A7 element is about the company's management and control of mobile storage media such as USB. A3 is about the HW or SW periodic upgrades and maintenance of ships' computers. A4 is about updates of anti-virus and anti-malware SW, and A2 is about restrictions on onboard security access to visitors. These items can be easily implemented using a small budget if the company is interested in cybersecurity.

On the other hand, A8 (3.03 points), A1 (3.42 points), and A9 (3.45 points) elements get relatively loss vulnerability scores. These elements are about disposal policy of ship’s equipment, training and awareness education onboard and land personnel for cybersecurity, the establishment of cyberattack contingency plan. They require a

relatively high level of understanding and analysis of ship cybersecurity to implement cybersecurity measures properly.

There was also a gab of security vulnerabilities between large shipping companies and small companies in the Administrative Security part. In particular, small shipping companies had a very low-security vulnerability score of 2.6 points in the A1 element, which corresponds to enhancing employee education and awareness for cybersecurity. Effective education and awareness of cybersecurity require long-term professional improvement and efforts by the staff in charge and the development of appropriate teaching materials. However, using outside experts could affect progress in the short term.

6.2.3. Technical Security Analysis

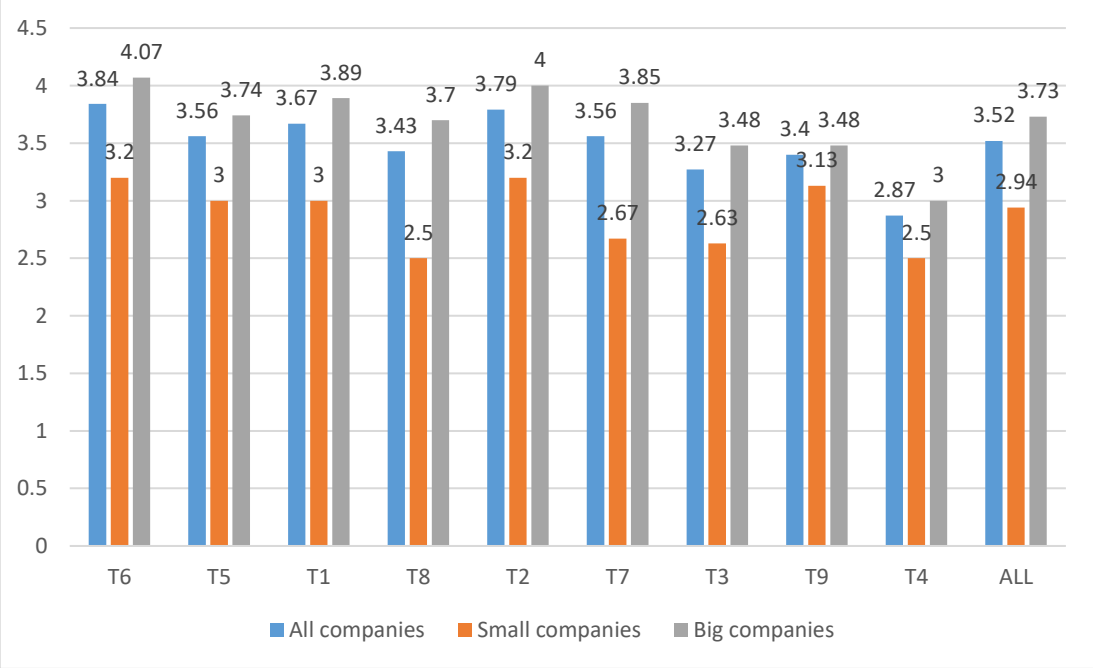
In Table 12 below, the cybersecurity elements of the Technical Security part are listed in order of higher risk values, with the highest risk value of 3-2-1 (T6) element and the lowest risk value 3-2-9 (T4) element. Figure 12 shows the vulnerability analysis results for cybersecurity elements in Table 12.

Table 12. Technical Security items & Identification code

Cybersecurity elements	Identification Code
3-2-1. Anti-malware software is installed on ships' computers, and periodic patch file updates are made.	T6
3-2-2. Remote access control is performed on a ship's networks and computers using an encryption key.	T5
3-2-3. Network ports, protocols, and services of ship’s networks and computers are restricted and controlled.	T1

3-2-4. Protection is being provided for e-mail and web browsers with wired and wireless access to ships' computers.	T8
3-2-5. Network devices such as firewalls, routers, and switches are configured to protect networks and computers on board.	T2
3-2-6. Security configurations of hardware and software (restrictions on access to systems outside of control) are being implemented.	T7
3-2-7. Cyberattacks detection, prevention, and warning are being made through the system for onboard networks and computers.	T3
3-2-8. Support for data backup and recovery is provided for onboard computers.	T9
3-2-9. Data encryption is taking place through the use of virtual private networks (VPNs) to connect to onboard networks.	T4

Figure 12. Cybersecurity Vulnerability of Korean Shipping Companies (TS Part)



The overall vulnerability value of the Technical Security part is 3.52 points, which is the middle of the three security parts. Among elements of TS part, T6 (3.84 points) and T2 (3.79 points) scored relatively high. T6 item is for installation and periodic patching of anti-malware software, and T2 is for configuration of network devices such as firewalls, routers, and switches.

On the other hand, the T4 (2.87 points) element on data encryption through virtual private networks (VPNs) received noticeably lower scores, which seems to reflect the reality that VPN is difficult to apply to existing networks of ships. Analysis results of the company's size showed that the security vulnerability scores of large companies were much better. However, it is difficult to understand those small companies have the lowest scores for relatively easy-to-action e-mail and web browser protection (T8) element in the field of technical security.

6.2.4. Physical Security Analysis

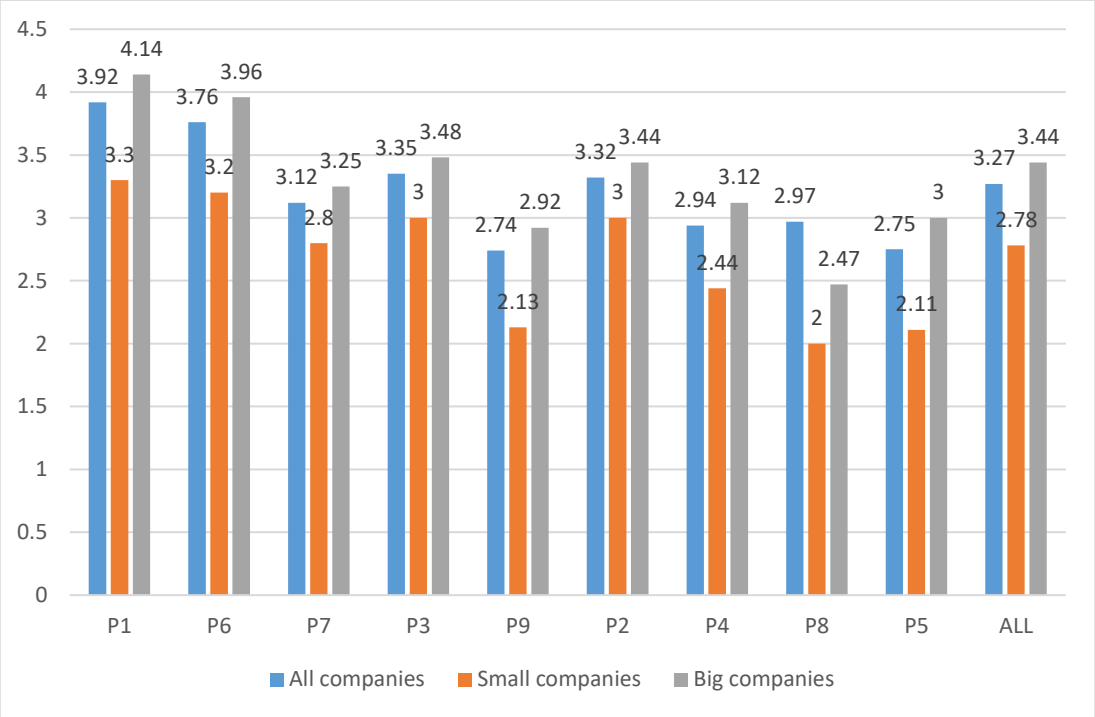
Physical security is a part of determining the status of physical protection measures such as markings, blockers, locks, etc. in the area to protect the ship's main facilities, equipment, and information. In order to strengthen the physical security of existing ships, the company may be burdened with costs due to the need to change and reinforce the ship's structures or facilities

Table 13. Physical Security items & Identification code

Cybersecurity elements	Identification code
3-3-1. Physical security zones and access control are in place for important facilities on board.	P1

3-3-2. Equipment, information, and software are prohibited from being taken out without prior approval.	P6
3-3-3. Procedures are being implemented to remove and verify data and license S/W in the event of reuse and disposal of equipment, including storage media.	P7
3-3-4. Control of unauthorized user access and isolation procedures for an information system is being implemented	P3
3-3-5. A policy of desk-cleaning for papers, portable storage media is being implemented.	P9
3-3-6. Physical security design and application to the ship's offices, workspaces, and critical facilities are being implemented.	P2
3-3-7. Procedures are being implemented to ensure continuous availability and confidentiality of equipment from the shutdown of the ship’s electric power and support facilities.	P4
3-3-8. Procedures for verifying the protection and management of users' information on unused equipment are being implemented.	P8
3-3-9. Procedures are being implemented to protect power and communication cables that support data transmission and information facilities.	P5

Figure 13. Cybersecurity Vulnerability of Korean Shipping Companies (PS Part)



The Physical Security part received the lowest overall score among the three parts of security vulnerability assessments. However, P1 scored 3.9 points, higher than A3, A4 items (3.89) in the administrative part and T6 item (3.84) in the technical field, which has higher overall scores than the physical security part. This is believed to be because item P1 is quite similar to physical security zone establishment and access control measures of the ISPS Code already in place. On the other hand, P9 scored 2.74, the lowest among 27 security vulnerability assessment elements. P9 is very simple to store documents and portable storage media that need security management in the ship's bridge or office in storage facilities with locks after use. However, due to the lack of awareness of security management of documents or storage media used onboard, many companies do not seem to have taken appropriate measures.

In conclusion, the Korean shipping company's cybersecurity vulnerability to ships was relatively good. However, companies managing small vessels showed relatively

greater vulnerability in all security assessment items than companies managing large vessels. In particular, some small companies that manage ships under 5,000 GT were found to be more vulnerable.

Of the three cybersecurity assessment parts (Administrative, Technical, and Physical), the administrative cybersecurity part, which is related to the company's support and policy, got the highest ratings, while the physical sector, which requires relatively large resources, got the lowest ratings. On the other hand, it seemed necessary to raise awareness of security vulnerability in some items as there have been relatively low scores in the items where employees can take relatively simple measures, such as training (A1) and installation of locking devices for storage of cybersecurity materials (P9).

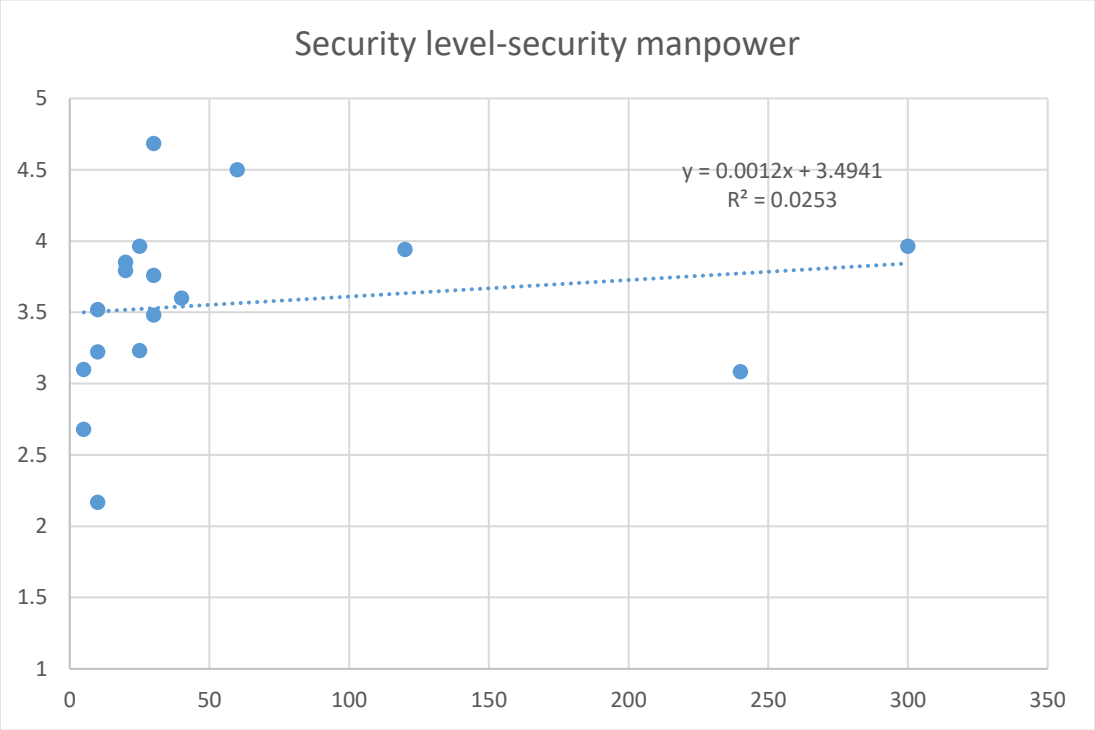
6.3. Correlation Analysis

In the previous chapter, cybersecurity vulnerabilities were reviewed from the perspective of cybersecurity elements for each company. This chapter analyzes what factors these cybersecurity vulnerabilities correlate with within the company.

6.3.1. Correlation between cybersecurity manpower and cybersecurity vulnerabilities

In chapter 6.1.3, we looked at the current status of cybersecurity personnel of the companies. It is meaningful to analyze the relevance between cybersecurity personnel and the company's cybersecurity vulnerabilities because each company has a large deviation in the cybersecurity workforce, and the organization's workforce is a crucial factor in identifying the level of work

Figure 14. Correlation between Manpower and vulnerabilities



The horizontal (X) axis is the manpower value[4] of the security personnel. The vertical(Y) axis is a cybersecurity vulnerability value of companies calculated in Chapter 6.2, expressed here as a security level. The lowest point on the security level is one, and the highest point is five.

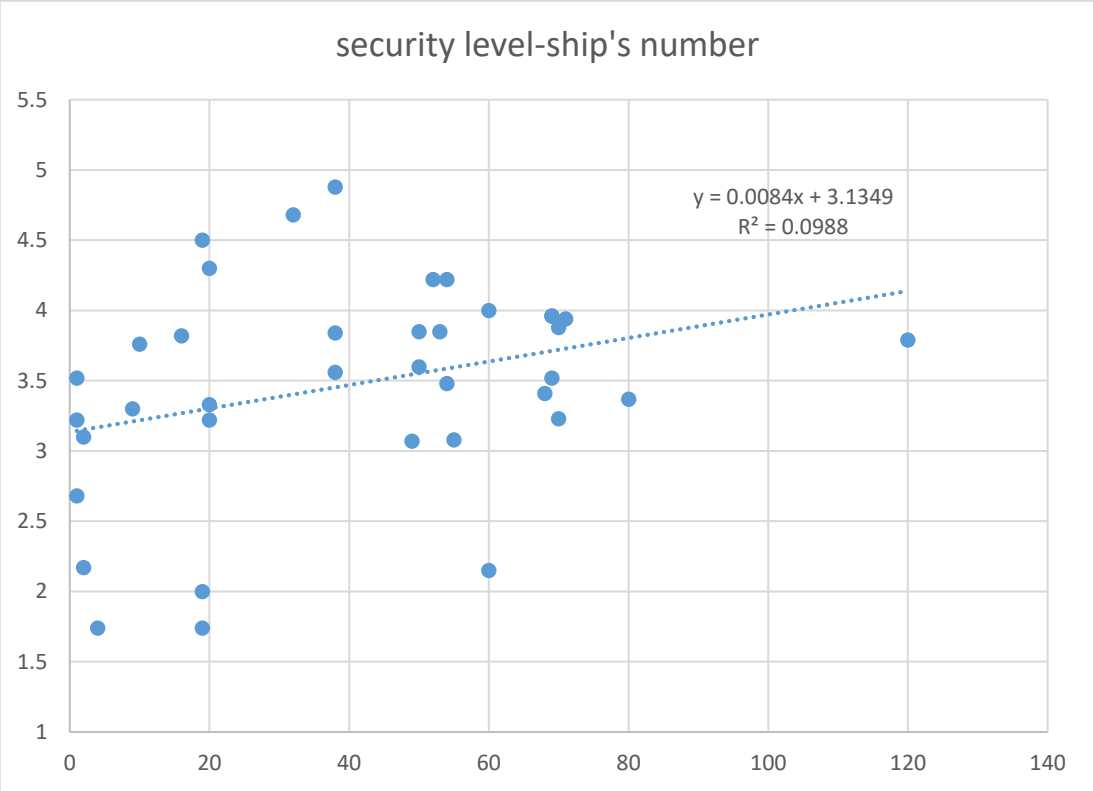
In this graph, the Coefficient of Determination (R^2) was 0.0253, resulting in a Pearson Correlation Coefficient(R) of 0.15906. By Table 5 standards, 'Weak correlation' exists between security personnel manpower and the company's security vulnerabilities, and the contribution to security vulnerabilities of security manpower is only 2.53%.

[4] The manpower value was calculated by multiplying the company's security personnel index by 100. The security personnel index is calculated by multiplying the total number of security managers by the dedicated rate, and the 1 dedicated personnel index means that one security manager performs security work eight hours a day. For example, if the company has four dedicated personnel and the average dedicated rate is 20%, the dedicated personnel index is 0.8 and the manpower value is 80. The manpower value is only to improve the visibility of the graph.

6.3.2. Correlation between ship's number and cybersecurity vulnerabilities

Usually, suppose the company has a large number of management vessels. In that case, it can be expected that the level of management of the vessel, including cybersecurity, will be high because sufficient management resources (personnel, budget) can be invested. Here, the correlation between the number of managed vessels and the cybersecurity vulnerabilities of individual companies is analyzed.

Figure 15. Correlation between ship's number and vulnerabilities



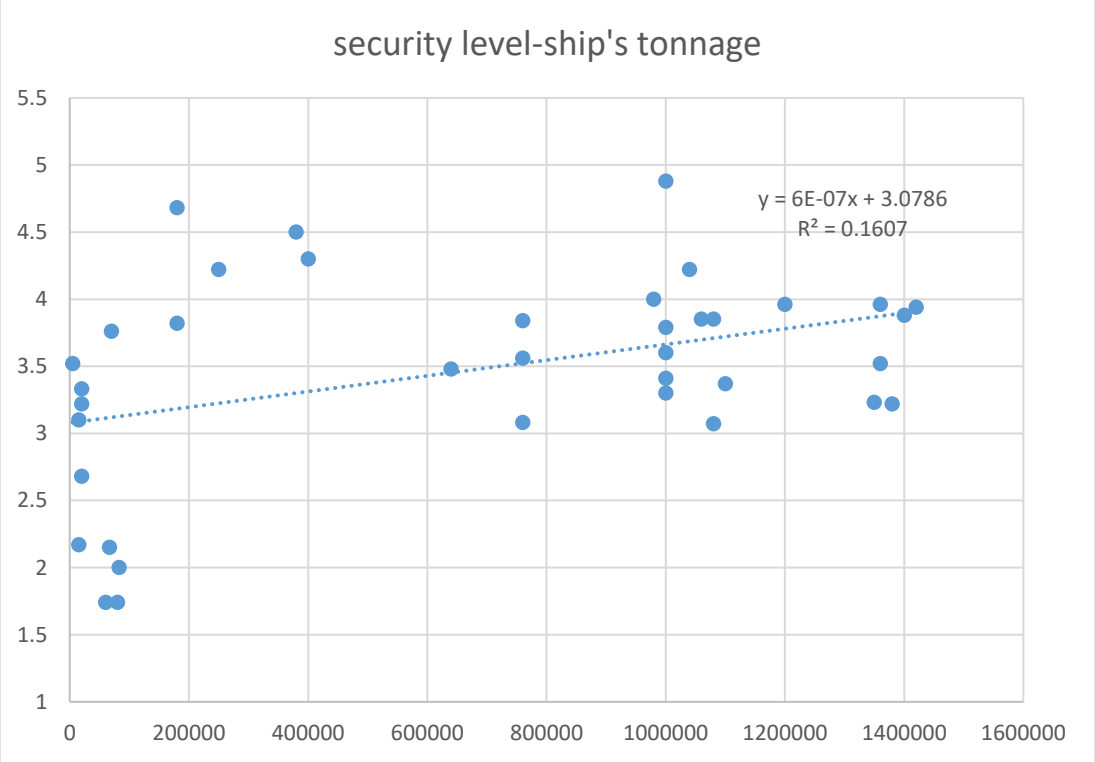
The X-axis is the number of managed vessels of a company, and the Y-axis is the company-specific cybersecurity vulnerability value calculated in Chapter 6.2. Here, the coefficient of determination $R^2 = 0.0988$ and a Pearson Correlation Coefficient $R = 0.314325$. In accordance with Table 5, the correlation between the number of

managed ships and cybersecurity vulnerabilities was 'Weak correlation', and the contribution of the number of ships to determine security vulnerabilities was 9.88%.

6.3.3. Correlation between Total Tonnage scale and cybersecurity Vulnerabilities

When judging the size of the company's management vessels, it is difficult to rely simply on the number of ships. This is because it cannot be said that a company that manages ten ships with 500 Gross tons is larger than a company that manages two ships with 100,000 Gross tons. So here, the correlation between the companies' security vulnerabilities and the total Gross tonnage of all vessels managed by the company is analyzed.

Figure 16. Correlation between ship's tonnage and vulnerabilities



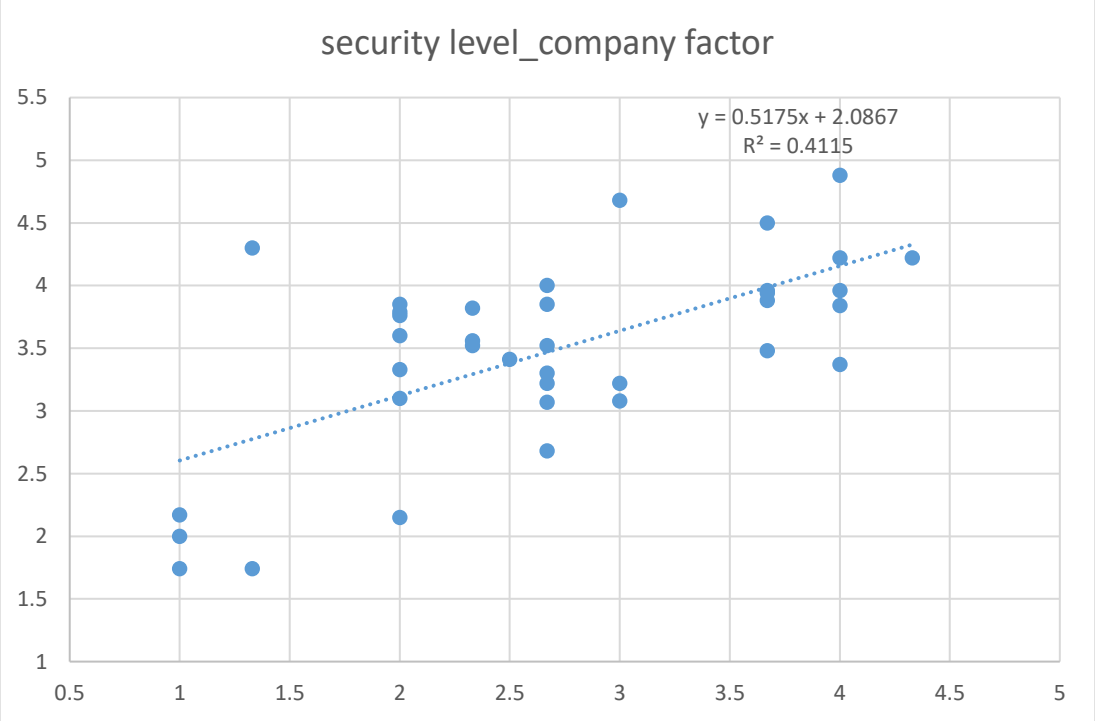
The X-axis represents the sum of the total GT of all vessels held by a company, and the Y-axis represents the company's security vulnerability value calculated in Chapter

6.2. The correlation between the total tonnage of the vessel and the security vulnerability resulted in a determination coefficient R^2 = 0.1607 and a Pearson correlation coefficient R = 0.4009. According to Table 5, the total tonnage of managed vessels and the company's security vulnerability relationship have a 'Moderate correlation' relationship. The contribution of total GT for company's cybersecurity vulnerabilities is about 16.1%.

6.3.4. Correlation between company's cybersecurity capabilities and cybersecurity vulnerabilities

Chapter 6.1.4 identifies the company's cybersecurity response capabilities in three areas: organization & human resources, employee expertise, education & training. Here it will be revealed how each company's cybersecurity response capabilities correspond to the company's cybersecurity vulnerabilities.

Figure 17. Correlation between company factor and vulnerabilities



The X-axis is a minimum of 1 point and a maximum of 5 points for the company's cybersecurity response capability in three areas: organization & human resource, workforce, expertise, education & training. The Y-axis is the value of a company's cybersecurity vulnerability calculated in paragraph 6.2. This scatterplot was also shown as R^2 = 0.4115 on the trend line and calculated as the Pearson correlation coefficient R =0.641483. According to Table 5, the correlation between the company's cybersecurity response capabilities and the company's cybersecurity vulnerabilities is a 'Moderate correlation,' with 41.15% contributing to the company's cybersecurity vulnerability values.

In addition, the relationship between each of the three elements of the companies' cybersecurity response capabilities and the company's cybersecurity vulnerabilities can be found in Table 14. Of the three company capabilities items, organizations & personnel had the highest relevance to the company's cybersecurity vulnerabilities, and education & training had the lowest relevance. However, it can be seen that the company's overall capability, which combines the three components, has the greatest relevance to the company's security vulnerabilities.

Table 14. Correlation values of company factors

	organizational & human resources	expertise	Education & training	Total
R^2	0.3095	0.2666	0.226	0.4115
R	0.556327	0.516333	0.475395	0.641483
Level of correlation	Moderate correlation	Moderate correlation	Moderate correlation	Moderate correlation

7. Discussion and Conclusion

7.1. Discussion of Findings

In this chapter, we will discuss the characteristics of the cybersecurity of Korean shipping companies discovered through the analysis of Chapter 6 and discuss possible improvement measures.

The overall score for cybersecurity vulnerabilities of Korean shipping companies was 3.47, which was found to be relatively reliable. According to the vulnerability rating table in Table 4, 3.47 points belong to the Invulnerable section. In a survey of companies' general status, most companies were aware of IMO resolution 428, and about 87% of respondents said they had established a ship cybersecurity management procedure at the company level. Nevertheless, companies with an average ship’s size of less than 10,000 GT showed relative vulnerability with an overall score of 2.9 points. Therefore, it seems desirable to focus mainly on small companies for IMO or national-level efforts in response to future cybersecurity threats

Among the three areas of cybersecurity elements, the vulnerability of the administrative security part got the highest score with 3.65 points, and the vulnerability of the physical security part was the lowest with 3.27 points. The high score in the administrative security part is believed to be due to the completion of the establishment of management procedures for the cybersecurity of ships in most companies and the maintenance of policy support. On the other hand, in some cases, the physical security part requires changes in the ship's facilities or structure, so it seems that companies have not taken active action yet. However, measures such as removing S/W licenses (P7) or user information (P8) of equipment discarded or storing (P9) in drawers with key security documents after use (P9) may be implemented at no additional cost.

Of the 27 cybersecurity elements, Vulnerable or Very Vulnerabe rating in Table 4(the vulnerability rating table) is only one element(P8). However, in the case of small

shipping companies, the following six elements were found to be vulnerable or very vulnerable rating.

- T4: Data encryption is taking place through the use of virtual private networks (VPNs) to connect to onboard networks (low risk).

- T8: Protection is being provided for e-mail and web browsers with wired and wireless access to ships' computers (medium risk).

- P4: Data encryption is taking place through the use of virtual private networks (VPNs) to connect to onboard networks (low risk).

- P5: Procedures are being implemented to protect power and communication cables that support data transmission and information (low risk).

- P8: Procedures for verifying the protection and management of users' information on unused equipment are being implemented (low risk).

- P9: A policy of desk-cleaning for papers, portable storage media is being implemented (medium risk).

T4, P4, P5, and P9 belong to the low-risk domain at the risk level in Figure 2, so even if the company's cybersecurity management system is somewhat weak, it may not be a big threat in terms of the overall aspect. However, the risks of T8 and P9 can pose a practical threat to cybersecurity management because they belong to medium risk with high probability and severity. Therefore, the government or related organizations, such as Class, need first to guide companies to strengthen these two elements.

As a result of analyzing the correlation between the company's cybersecurity vulnerability and the company's four characteristics (cybersecurity manpower, number of ships, total tonnage of ships, and company’s cybersecurity capabilities), manpower and ship’s number showed the Weak Correlation, and total tonnage and the company's capability showed the Moderate Correlation according to Table 5. In

particular, the company's cybersecurity capabilities had the greatest correlation with vulnerability. Therefore, in order to improve the company's cybersecurity vulnerability, it is desirable to improve the company's capabilities related to cybersecurity rather than simply increasing the number of cybersecurity managers.

The company's cybersecurity capabilities are divided into three areas: organization & human resources, employee expertise, education & training, of which organization & human resources had the greatest correlation with vulnerability. However, organically combining three items rather than individual items had a more significant correlation with vulnerability. Therefore, the enhancement of the company's cybersecurity capabilities needs to be comprehensively improved across all fields, such as organization, expertise, and education, rather than focusing on any one field.

7.2. Conclusion

In Chapter 4, it was confirmed that cyber threats are rapidly increasing due to the development of technology following the Fourth Industrial Revolution and the strengthening of the connectivity between informatization devices. In addition, Chapter 5 predicts that cybercrime is frequently occurring in the maritime industry, which has been a safety zone for cyber threats so far, and that cyber threats will be the biggest issue in the next decade with the introduction of advanced ICT technologies such as e-Navigation and Autonomous ships

Related organizations such as BIMCO, Oil Majors, and Bulk Shipper Associations, led by IMO, have been making efforts to publish cybersecurity guidelines, integrate cybersecurity regulations into ships' SMS, and include cybersecurity elements in shipper inspections' items for oil tankers and bulk ships.

This paper analyzed how the efforts of these related agencies are being implemented in the field of the shipping industry through the evaluation of the cybersecurity vulnerability of shipping companies. In addition, in order to find ways to strengthen cybersecurity vulnerabilities, it was analyzed how the vulnerability of shipping companies correlates with various company characteristics.

The first research question in Chapter 1.3 concerns the implementation of cybersecurity elements of shipping companies. In Chapter 6.2, it was analyzed that Korean shipping companies are relatively well implementing important cybersecurity elements of cybersecurity guidelines issued by BIMCO and others. On the other hand, it was confirmed that the deviation of cybersecurity vulnerabilities between individual companies was large, and the security vulnerability of the small company group was 2.9 points, which was considerably lower than that of the large company group 3.69 points.

Regarding the second research question, Chapter 6.3 analyzed the correlation between cybersecurity vulnerabilities and company characteristics. Here, it was confirmed that the company's cybersecurity capabilities had the greatest correlation with vulnerabilities, and the number of cybersecurity managers or management ships had a relatively low correlation with cybersecurity vulnerabilities.

Regarding the third research question about IMO and States' strategies to improve cybersecurity vulnerabilities, based on the results of the discussion in Chapter 7.1 and the results of the previous two research questions, it is judged that the following suggestions are possible.

First, it is necessary to clarify the target of the policy. As can be seen from the analysis in Chapter 6.3, It is common for the vulnerability of the entire group to differ greatly between individual companies or specific groups. Small shipping companies are more likely to be vulnerable than large shipping companies, and companies that manage general cargo ships lines are more likely to be vulnerable than companies that manage oil tankers or bulk carriers which are inspected by the shipper associations. In addition, Domestic shipping companies are more likely to be vulnerable than international shipping companies. Therefore, in order to effectively utilize the limited resources of the government or international organizations, it is desirable to focus on more vulnerable areas and promote policies to improve cybersecurity vulnerability.

Second, it is necessary to clarify and simplify cybersecurity elements that companies must comply with. The contents of the security guidelines published by BIMCO or ISO/IEC are vast and professional, making it difficult for ordinary employees to understand. Most shipping companies, regardless of the size of the company, received low vulnerability scores in P8 item on user information protection of unused equipment and P9 item to store critical data used in on board offices in drawers with locked devices. This is believed to be due to companies' poor identification of these two items hidden in the vast cybersecurity guidelines because it is not so difficult to implement these items. Therefore, making cybersecurity elements that companies must comply with simple and straightforward can increase the level of cybersecurity response of companies.

Third, cybersecurity should be considered from the time the ship is designed. Among cybersecurity elements, T4 (2.87 points), P4 (2.94 points), and P5 (2.75 points), which require facility or structure changes, received lower scores than average (3.47 points), but It takes a lot of time and money to improve these items. Therefore, there is a problem that it cannot be easily improved after the ship is built. Moreover, if e-navigation or automatic ships increase in the future, direct cybersecurity threats to ships will increase significantly. Therefore, it is desirable to add cybersecurity regulations to IMO's shipbuilding standards from now on.

Finally, the increase in cyber pirates and terrorism using ships can have a much more serious impact than we expect. As the application of ICT technology to ships and the universal use of the Internet using satellites become more common, cyber threats to ships will increase day by day. Therefore, it is time for interested organizations such as IMO, each member state, and BIMCO to once again check the effects of current cybersecurity response policies and come up with more effective strategies. Moreover, cybersecurity response at the global level is a goal that cannot be achieved by the shipping companies or one country level. Therefore, international cooperation and efforts centered on IMO should continue to strengthen cybersecurity.

7.3. Limitations

In order to accurately grasp the cybersecurity response situation of the maritime industry around the world, it is desirable to investigate various countries such as developing countries, developed countries, shippers' countries, and shipowners' countries.

In addition, the cybersecurity elements used in this paper are mainly intended to confirm the status of the operational elements of cybersecurity in terms of managing ships. However, cyberattacks use a variety of routes connected to the target. Therefore, in order to substantially secure the cybersecurity of the ship, the security status of various targets connected to the ship must be analyzed. In other words, it is necessary to review cybersecurity vulnerabilities across the maritime industry, including port and terminal operating companies, shipping companies' land departments, shipping agencies, quarantine stations, customs, VTSs, and shippers.

However, as explained in Chapter 1.4 of the study, the scope of this paper was limited to analyzing the compliance of Korean shipping companies with ship cybersecurity elements and the correlation between the company's characteristics and cybersecurity vulnerabilities due to time and data constraints. Moreover, it is true that the average analysis results were evaluated somewhat higher than the actual situation due to the very low response rate of small ship companies that are presumed to be poor in the operation of cybersecurity in the survey of shipping companies. Nevertheless, this paper will be meaningful in that it is possible to understand how cybersecurity guidelines developed by BIMCO are being implemented in the field. Moreover, it is believed that analyzing how vulnerabilities derived from cybersecurity operations correlate with the various characteristics of the company could serve as a guide for IMO or member states to establish cybersecurity-related policies in the future.

References

Adebayo, A. O., Chaubey, M. S., & Numbu, L. P. (2019). Industry 4.0: The Fourth Industrial Revolution and How IT Relates to The Application of Internet of Things (IoT). *Journal of Multidisciplinary Engineering Science Studies (JMESS)*, 5(2), 2477-2482.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, 8(10), 776. https://doi.org/10.3390/jmse8100776

Beaming. (2020). Five Years in Cyber Security (Cyber Report). https://www.beaming.co.uk/cyber-reports/five-years-in-cyber-security-report/

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC). (2020). *The Guidelines on Cyber Security Onboard Ships [Version 4]*. BIMCO.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13–21. http://timreview.ca/article/835

Do, S. R. (2019) 사이버 보안 표준 및 위협 분석 기법 동향. *주간기술동향 1918 호*, 2-15. 정보통신기획평가원.

Enders, F.B. (2020, May 26) Coefficient of determination. Encyclopedia Britannica. https://www.britannica.com/science/coefficient-of-determination.

Ha, Y.W. (2019) 사이버범죄 대응을 위한 국가지능화 적용 방향, *ETRI (Electrics and Telecommunication Research Institute) Insight Report 2019-25*. ETRI.

International Maritime Organization [IMO]. (2017, June 16) *Maritime Cyber Risk Management in Safety Management System* (Res. MSC.428(98)).

Jo, Y. H., & Cha, Y. K. (2019). A Study on Cyber Security Requirements of Ship Using Threat Modeling. *Journal of the Korea Institute of Information Security & Cryptology*, 29(3), 657-673. https://doi.org/10.13089/JKIISC.2019.29.3.657

Kim, H. C., Choi, S. K., & Choi, D. H. (2016). A simulation comparison on the analyzing methods of Likert type data. *Journal of the Korean Data and Information Science Society*, 27(2), 373–380. https://doi.org/10.7465/jkdi.2016.27.2.373

Kim, H. K., Choi, B., Ko, E., & Park, S. (2019). 5G 네트워크 기술 진화에 따른 새로운 5G 보안 도전과제와 해외 보안 아키텍처 연구 동향. *Review of Korea Institute of Information Security and Cryptology(KIISC)*, 29(5), 7-20.

Kim, J. S., & Lee, M. H. (2018). 5G Mobile Communications: 4th Industrial Aorta, *The Journal of the Convergence on Culture Technology (JCCT)*, 4(1), 337–351. https://doi.org/10.17703/JCCT.2018.4.1.337

Km, S.H.& Kim, Y.H. (2019, March 30). 한국 유명선사 선박 수척 랜섬웨어 피해.. 사이버보안 경각심 가져야. *financialnews*. https://www.fnnews.com/news/ 201903300027281755

Korea Maritime Institute (2020) Development of Korean-flag Ocean-going Vessels. Shipping statistics handbook 2020. https://www.kmi.re.kr/web/contents/contentsView.do?rbsIdx =221

Lee, S.W. (2012) *A Study on the Effects of Safety Management System Factor on Management Performance of Shipping Company*. [Unpublished master's thesis]. Korea Maritime University

Morgan, S. (2020, Nov. 13) Cybercrime to cost the world $ 10.5 Trillion Annually by 2025 (Special Report:Cyberwarfare in The C-suite). *Cybercrime Magazine*.https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Park, Y.R. (2020, Oct. 5) 4 년 연속 해운기업에 사이버 공격, 이번엔 CMA CGM. S*hippers' Journal*. http://www.shippersjournal.com/mobile/article.html?no=26482

Park., H.S., Yoo, Y. J., Park, H. R (2019) *a Study on Strengthening Cybersecurity System in the Maritime Sector*. Korea Maritime Institute [KMI] . https://www.kmi.re.kr/web/board/view.do?rbsIdx=113&idx=37044

Patrick, S., Christa, B. & Lothar, A. S. (2018, May 1) *Correlation Coefficients: Appropriate Use and Interpretation.* Anesthesia & Analgesia, 126(5), pp. 1763-1768(6). https://doi.org/10.1213/ANE.0000000000002864

safety4sea (2020, July 20) *Cyber attacks on maritime OT systems increased 900% in last three years. https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/?__cf_chl_jschl_tk__=pmd_61QkenCwVLiTV.Kxz_exfYNMuQMmY.MdmI5zRPQtwYu4-1631188374-0-gqNtZGzNAiWjcnBszQi9&__cf_chl_jschl_tk__=pmd_IH_RAZsmGNKZPSOSavyl47y7ZU.nCdJbZIzpr0w4vS8-1632079614-0-gqNtZGzNArujcnBszQk9*

Song, J. S., 이혁로, 최상수, 황일선, 최윤수, 김진숙, ... & 송태욱. (2018). *최신 사이버위협 동향 및 대응 방안 분석 [인공지능 (AI) 을 활용한 보완관제 기술 고도화 중심].* Korea Institute of Science and Technology Information. https://doi.org/10.22810/2018KRR016

Starista (2021) Definition Interval scale. https://www.statista.com/statistics-glossary/definition/320/interval_scale/

Stokes, P., Baker, M. & Turner, R. (2018) Golbal Maritime Issues Monitor 2018 [PowerPoint slides]. https://www.globalmaritimeforum.org/content/2018/10/Global-Maritime-Issues-Monitor-2018.pdf

Swedish Civil Contingencies Agency (2012, March) Guide to risk and vulnerability. https://www.msb.se/RibData/Filer/pdf/26267.pdf

Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.

Tam, K., Jones, K. D., & Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. Eng. Technol. Ref, 1(5pp), 1-13.

Department of Homeland Security [DHS]. (2010, September) DHS Risk Lexicon 2010 Edition. https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

Warwick, A. (2018, FEB.). Economic impact of cyber crime is significant and rising. *ComputerWeekly*. https://www.computerweekly.com.

Wikipedia (2021, Aug.) Vulnerability. https://en.wikipedia.org/wiki/Vulnerability_(computing)

Wikipedia (2021, Aug.) Ordinal data. https://en.wikipedia.org/wiki/Ordinal_data

Wikipedia (2021, Aug.) 피어슨 상관 계수. https://ko.wikipedia.org/wiki/%ED%94%BC%EC%96%B4%EC%8A%A8_%EC%83%81%EA%B4%80_%EA%B3%84%EC%88%98

Yoo, Y.J. & Park, H.S. (2021. 24 May) Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. *Journal of Marine Science and Engineering*. 2021; 9(6):565. https://doi.org/10.3390/jmse9060565

.

Appendix 1

Questionnaires Survey for the vulnerability assessment of Korean shipping companies to cyber threats

Dear Participant,
This survey is design to assess the vulnerability of shipping companies to cyber threats. It is being conducted purely for academic research as part of my Master's Degree dissertation at the World Maritime University (WMU). It is not part of any privately or publicly funded project.

It will take about 40 minutes in providing responses to all the questions. It may also appear a bit tedious but please bear with me in completing the questionnaires.

If you have any questions, comments or suggestions about this survey, please feel free to contact me at w2005158@wmu.se or WhatsApp at number (+46)728337110.

Thank you very much for taking time to fill-in the questionnaires.

Yours sincerely.

Sungjae Kim
Student, Master of Science in Maritime Safety & Environmental Administration of World Maritime University, Malmo, Sweden

1. Personal particulars

Please answer the questions below about your personal information. Your personal information is being sought solely for purposes of record and validation of data, and will not be disclosed in any form

Questions	Answers
1-1. Name of participant	
1-2. Name of Company	
1-3 Kind of Company	(1) Ship owner (2) ship management company (3) others ( )

1-4. Your responsibilities in the Company	
1-5. Email address/telephone number	

2. General

Please answer the general question of your company. For multiple choice questions, you can choose the appropriate one out of the six answers.

<table>
<tr><th>Questions</th><th>Answers</th></tr>
<tr><td>2-1. Number of ships managed by your company</td><td></td></tr>
<tr><td colspan="2">In the following table, please indicate the size distribution of the ships managed by your company
<table>
<tr><td>Ship’s size (Gross Tonnage)</td><td>Less than 100 GT</td><td>100 GT or more ~ Less than 500 GT</td><td>500 GT or more ~ Less than 1000 GT</td><td>1000 GT or more ~ Less than 5000 GT</td><td>5000 GT or more ~ Less than 10000 GT</td><td>10000 GT or more</td></tr>
<tr><td>number of ships</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2-2. Did you know that the IMO Maritime Safety Commttee's Resolution on Marine Cyber Risk Management (IMO (2017.6), Resolution MSC.428 (98)) were implemented in January 2021?</td><td>Yes/No/Not applicable</td></tr>
<tr><td>2-3. Does your company incorporate cyber risk management regulations into its SMS according to the recommendations of the?</td><td>Yes/No/Not applicable</td></tr>
<tr><td>2-4. Does your company establish and implement procedures to prevent cyberattacks and crimes against ships?
* If you answered question 2–3 with yes, omit the answer.</td><td>Yes/No/Not applicable</td></tr>
<tr><td>2-5. Why does your company establish and implement cyberattacks (crime) prevention (response) procedures against ships?
* Answer questions when 2-3 or 2-4 answers are Yes (multiple responses available)</td><td>(1) PSC (2) Shipper’s request (3) cybercrime prevent (4) compliance with IMO or flag state recommendations (5) other( )</td></tr>
</table>

2-6. Number of ship security managers in the company	
2-7. Are your company's security managers exposed to work other than directly or indirectly related to ship security. If so, how many percent of their work do security managers use for work that is not related to ship security?	Yes/No %
2-8. Does your company have enough organization or manpower for ship security management?	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
2-9. Does your ship security managers have expertise in security work?	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
2-10. Are your security managers properly and periodically trained to improve ship security management?	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
2-11. What should your company first strengthen for effective ship security management (professionals, training, equipment, government support, etc.).	
2-12. Are there any external experts (or special company) contracted to perform your company's ship security management?	Yes / No
2-13. Do you think external experts (or special company) are doing enough for ship security management? (Answer only if the answer in 2-12. is yes)	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
2-14. What are the top priorities for external experts (or special company) to play an effective role (such as replacing experts, increasing staff, increasing contract amounts, etc.). (Answer only if the answer in 2-12. is yes)	

3. Ships Cybersecurity Management

Please answer questions about three areas (administrative, technical and Physical security) to investigate the current level of ship security management in your company.

These questions used data from a study on Strengthening Cyber-security System in the Maritime Sector (Korea Maritime Institute, 2019).

.**3-1**. **Administrative Security**

Questions	Answers
3-1-1. There is control over the mobile media (USB, mobile PCs, etc.) used in ships.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-2. Periodic upgrades and ongoing maintenance of H/W and S/W of ship computers* are performed.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-3. Trainings for ship and land staff are provided periodically to raise awareness on information protection.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-4. Anti-virus and anti-malware S/W tools supplied for ship computers.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-5. The policy of controlling remote access to ship computers is being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-6. Restricting access to ships (port officials, technicians, agents, etc) is being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-7. Access to sensitive information is granted only to authorized employees.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-8. Emergency plans are in place for cyberattacks.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-1-9. Equipment disposal policies, including data, are being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable

* ship computers mean all personal, business, and equipment control and operation computers (including those built into the equipment).

3-2. Technical Security

Questions	Answers
3-2-1. Anti-malware software is installed on ships' computers, and periodic patch file updates are made.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-2. Remote access control is performed on a ship's networks and computers using an encryption key.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-3. Network ports, protocols, and services of ship’s networks and computers are restricted and controlled.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-4. Protection is being provided for e-mail and web browsers with wired and wireless access to ships' computers..	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-5. Network devices such as firewalls, routers, and switches are configured to protect networks and computers on board.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-6. Security configurations of hardware and software (restrictions on access to systems outside of control) are being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-7. Cyberattacks detection, prevention, and warning are being made through the system for on-board networks and computers.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-8. Support for data backup and recovery is provided for onboard computers.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-2-9. Data encryption is taking place through the use of virtual private networks (VPNs) to connect to on-board networks.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable

3-3. Physical Security

Questions	Answers
3-3-1. Physical security zones and access control are in place for important facilities on board.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-2. Equipment, information and software are prohibited from being taken out without prior approval.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-3. Procedures are being implemented to remove and verify data and license S/W in the event of reuse and disposal of equipment, including storage media.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-4. Control of unauthorized user access and isolation procedures for information system are being implemented	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-5. A policy of desk-cleaning for papers, portable storage media is being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-6. Physical security design and application to the ship's offices, workspaces and critical facilities are being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-7. Procedures are being implemented to ensure continuous availability and confidentiality of equipment from the shutdown of ship’s electric power and support facilities.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-8. Procedures for verifying the protection and management of users' information on unused equipment are being implemented.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable
3-3-9. Procedures are being implemented to protect power and communication cables that support data transmission and information facilities.	(1) Strongly disagree (2) disagree (3) Neutral (4) Agree (5) Strongly agree (0) Not applicable

I would appreciate it if you could submit the completed questionnaire to w2005158@wmu.se