Journal of the Korean Society of Marine Environment & Safety
Research Paper
Vol. 27, No. 3, pp. 429-438, May 31, 2021, ISSN 1229-3431(Print) / ISSN 2287-3341(Online) https://doi.org/10.7837/kosomes.2021.27.3.429

Importance – Performance Analysis (IPA) of Cyber Security Management: Focused on ECDIS User Experience

Sangwon Park* · Yeeun Chang** · Youngsoo Park***†

* Senior researcher, Korea Maritime Institute, Busan, 49111, Korea
** Researcher, Marineworks, Busan 48792, Korea
*** Professor, Division of Navigation Convergence Studies, Korea Maritime & Ocean University, Busan 49112, Korea

Abstract : *The mandatory installation of the ECDIS (Electronic Chart Display and Information System) became an important navigational equipment for navigation officer. In addition, ECDIS is a key component of the ship's digitalization in conjunction with various navigational equipment. Meanwhile, cyber-attacks emerge as a new threat along with digitalization. Damage caused by cyber-attacks is also reported in the shipping sector, and IMO recommends that cybersecurity guidelines be developed and included in International Security Management (ISM). This study analyzed the cybersecurity hazards of ECDIS, where various navigational equipment are connected. To this end, Importance-Performance Analysis (IPA) was conducted on navigation officer using ECDIS. As a result, the development of technologies for cyber-attack detection and prevention should be priority. In addition, policies related to 'Hardware and Software upgrade', 'network access control', and 'data backup and recovery' were analyzed as contents to be maintained. This paper is significant in deriving risk factors from the perspective of ECDIS users and analyzing their priorities, and it is necessary to analyze various cyber-attacks that may occur on ships in the future.*

Key Words : *ECDIS, Cyber-attack, Security, Importance-Performance Analysis (IPA), digitalization*

1. Introduction

As the maritime industry has developed from the conventional ship era to the smart ship era, the reliance on digitalization, integration, and networking has grown. As technologies for shore have been developed, all interested parties have started to merge the technology into the maritime industry as e-navigation. However, as ships have been opened for satellite communications, the risk of cyber-attacks has increased significantly. Facing new issues, IMO (International Maritime Organization) and other organizations established guidelines for cyber security (IMO, 2016; IMO, 2017; OCIMF, 2017; BIMCO, 2018).

In the 86th session of the IMO Maritime Safety Committee (MSC), the SOLAS amendment was adopted to use ECDIS as the main navigation system, and it was mandatory to mount ECDIS from 2012 to 2018 (IMO, 2009a; IMO, 2009b). ECDIS, which has been mounted as a navigation device, is now an important device along with changes in the digitalization environment (Kwon et al., 2021).

Jung et al. (2015) suggested improvements in ECDIS function in terms of navigation safety and efficiency through a survey of officers. Lee (2018) conducted a user evaluation of ECDIS, which has become essential equipment for ships; and found that the efficiency of work simplification and cost reduction declined immensely after usage. It was suggested that not only is user education necessary but also a change in the system level. Lee et al. (2019) analyzed ECDIS-related accident reports using text-mining techniques; and found that accidents related to ECDIS problems are increasing. Kwon et al. (2021) evaluated the relative importance of the bridge navigation equipment through AHP analysis and found that RADAR, GPS, and ECDIS were relatively important and had a large impact on maritime accidents. Current ECDIS research focuses on user-oriented operation and navigational safety.

Regarding security in the maritime field, KMI (2019) analyzed the policies of major countries on cyber risk management in the maritime field and presented policies related to maritime cyber security through a survey. D'agostini and Jo (2019) concluded with the fact that security training for seafarers has a positive effect on seafarers' security awareness and ship security performance. Lee et al. (2020) suggested designating a ship's cyber security officer and opening a class for training courses. Svilicic et al. (2018) proposed a risk assessment framework based on an on-board survey, and

* First Author : psw6745@kmi.re.kr, 051-797-4919
† Corresponding Author : youngsoo@kmou.ac.kr, 051-410-5085

conducted a risk assessment for ECDIS using a vulnerability-scanning tool according to the proposed framework. Until now, most studies have focused on the importance of ship cyber security and the importance and connectivity of ECDIS as a navigation device. However, Svilicic et al. (2018) conducted an ECDIS risk assessment related to ship cyber security, however, it focused on overall security. This study is significant in that policy priorities are proposed by quantitatively indicating the importance and performance level of ship cyber security risk factors of ECDIS based on user experience. In other words, the purpose of this study was to establish the ECDIS cyber security risk factors from the user's perspective and to present policy priorities through quantitative analysis. This study analyzed the cyber security risk factors of ECDIS, which is the key equipment for ship digitization. The trend of cyber security in the maritime sector was analyzed, and cyber security-related policies that should be prioritized through an importance-performance analysis of officers who are actual users of ECDIS.

2. Overview of ECDIS Cyber Security

2.1 Trend of Cyber Security

As IMO is responsible for the safety and security of shipping, they announced that cyber security technology will be the main subject and will focus on cyber security until 2023. In this regard, IMO also showed the urgent need to raise awareness of cyber risk threats in the maritime field and its vulnerabilities.

The IMO has established guidelines on maritime cyber risk management (MSC-FAL.1/circ.3). The document; states that their maritime cyber risk management goal is to support safe and secure shipping, which is operationally resilient to cyber risks. Therefore, the MSC at its 98th session in June 2017 adopted Resolution MSC.428 (98) – Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after January 1 2021. Additionally, the IMO has also imposed high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

The IMO's guidelines present the following functional elements that support effective cyber risk management.

Table 1. Elements of the cyber security in IMO guidelines

Identify	Define personnel roles and responsibilities for cyber risk management and identify systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations.
Protect	Implement risk control processes measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
Detect	Develop and implement activities necessary to detect a cyber-event in a timely manner
Respond	Develop and implement activities and plans to provide resilience and restore systems necessary for shipping operations or services, which get impaired due to a cyber-event.
Recover	Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

2.2 BIMCO

BIMCO, the world's largest direct-membership organization of ship-owners, charterers, shipbrokers, and agents, has also published guidelines on cyber security onboard ships. The purpose of these guidelines is to improve the safety and security of seafarers, the environment, cargo, and ships.

Published guidelines aim to assist in the development of a proper cyber risk management strategy following relevant regulations and best practices on board a ship with a focus on work processes, equipment, training, incident response, and recovery management.

The 4th guidelines for ship cyber security were published in 2019 and provide ship-owners and operators with guidelines and procedures to secure the company's cyber systems.

2.3 Case Studies

As the era of autonomous ships has arrived, the maritime industry is constantly evolving. One of the biggest changes in ships is that the system has changed into an interconnection of networks between the navigation equipment. Kesseler et al. (2019) mentioned that the interconnectedness of networks within a system allows one network to provide a path to other networks. As various equipment are interconnected, it is now much easier for hackers to access the data. Below are examples of cyber-attack cases in the maritime field, which demonstrate the damage that can be caused.

(1) A.P. Moller Maersk

In 2017, Maersk was infected by the Ukrainian tax return vendor MeDoc. The virus was spread across the entire company's IT network within seven minutes, including all core business units. Consequently, the company's booking website and 49,000 laptops were destroyed, 1,200 apps were instantly inaccessible and 1,000 applications were disrupted. Since the virus spread rapidly, the company had to disconnect immediately from the global network and revert to manual systems.

After reverting to a manual system, trading volumes reduced by 20%, and online bookings were only resumed after eight days. After four weeks, the full IT network was restored and the Maersk line had to re-install 45,000 PCs and recover 4,000 server applications. Consequently, the NotPetya attack caused a $300M financial loss.

The NotPetya ransom ware which was used in this attack, had a history of inflicting widespread damage not only against the FedEx system of an air logistics company but also throughout companies in Ukraine. NotPetya is a malicious code, which runs on the Windows operating system, as a variant of the ransom ware Petya, which exploits Windows Server Message (SMB) vulnerability to encrypt the entire Master Boot Record file and requires bit coin for the decryption cost. NotPetya was more lethal than Petya as it was impossible to recover encrypted data.

(2) Iranian Shipping Line

In 2011, the Islamic Republic of Iran Shipping Line (IRISL)'s server was subjected to cyber-attacks. In 2011, IRISL had the largest fleet in the Middle East consisting of 170 ships. Due to the attack, the company lost all data for their fleets, including rates, loading information, cargo tracking numbers, and customer information. This meant that nobody knew which container should be delivered to where or whom, whether the cargo had been loaded or not, and which containers were left on board.

Furthermore, the attack continued to eliminate the company's internal communication network. This caused significant disruptions in operations and resulted in sending cargo to wrong destinations causing severe financial losses.

(3) Mediterranean Shipping Company (MSC) shipping

The Mediterranean Shipping Company, which has over 480 offices across 155 countries worldwide, was cyber-attacked on April 9, 2020. The attack disrupted the company's global services by file-encrypting malware, causing a data center outage and leading to main customer's websites being down for days.

MSC shipping confirmed that it was confined to a limited number of physical computer systems in Geneva only and determined that it was a malware attack based on an engineered targeted vulnerability.

(4) ECDIS Cyber-attack

Most vessels receive their updated electronic navigational chart (ENC) or update ECDIS software through USB or CD/DVD. Officers are predominantly unaware of the fact that a USB/CD/DVD could be infected with a virus and plugged it without scanning for any viruses. For example, during an inspection onboard a tanker, the inspector noticed that a USB drive was plugged into the ECDIS to install updates for ENCs. The officer of the watch complained that the system was too slow and some false alerts popped up on the ECDIS computer, creating an abnormal system. Fortunately, with the assistance of the inspector and the managing company's IT department, it was found that ECDIS sensor data were manipulated with unreliable information displayed to the officer of the watch.

Kesseler et al. (2019) introduced a case of an ECDIS attacked by malware that was inserted into the vessel's ECDIS through a satellite link. As many vessels are open to satellite communication and have internet access, the malware was inserted into the vessel's electronic chart display information system via a satellite link to the master computer. The malware altered the ship's position during the night without changing the ECDIS display. The second piece of malware was uploaded to the radar system via a network switch that connected radar, ECDIS, bridge, and other ship communication systems. This malware altered the radar display by deleting targets on the display, essentially blinding the ship. The final malware was inserted into the machinery control systems network via an infected thumb drive.

As ECDIS is receives many data signals through various equipment, it has been proven that the ECDIS is highly vulnerable to attacks such as malware via computer viruses, worms, Trojan horses, or ransom ware. To protect the ECDIS from cyber-attacks, access should be restricted to only trained and authorized personnel including computer operation system (OS) and password protection.

2.4 ECDIS

(1) Entry into the ECDIS

Since 2002, vessels have had the option to be fitted with an ECDIS along with a backup arrangement as a means of fulfilling the requirement under the International Convention for the Safety of Life at Sea (SOLAS, 1974) regulation V/19-2.1.4 for the vessel to carry nautical charts for the intended voyage.

This option is now transforming into a mandatory requirement as at a meeting of the IMO MSC in May and June 2009, further amendments to SOLAS regulation V/19 were made to make the carriage of an ECDIS mandatory on vessels engaged in international voyages with an expected date of entry into force as of January 1, 2011.

According to on-board fulfillment requirements, Svilicic et al. (2019) stated that the ECDIS must be type-approved, with up-to-date ENCs implemented, ECDIS software maintained, and an adequate backup arrangement installed (IMO, 2017; IMO, 2006; IHO, 2017; IHO, 2018). Svilicic et al. (2019) explained that an ECDIS is considered a critical operational technology for voyage planning which complies with the updated paper charts (complies with IMO regulations and mandatory carriage) and plays a central role in safe ship navigation and transport (IMO, 2017).

(2) ECDIS function

The primary function of an ECDIS is to not only replace paper charts but also to contribute to safe navigation by receiving and displaying information from other navigational equipment. The main functions supported by an ECDIS are as follows:

- Displays the ship's speed
- Displays own ship information based on GPS coordinates
- Plans the route through the route planning function
- Monitors the route
- Displays alarms and warnings when a dangerous object approaches or when entering a dangerous area
- Records the track and information of the ship
- Displays AIS target information
- Radar overlay

According to the IMO performance standards, the system should be directly connected to three sensors mandatorily: position, heading, and speed. However, as time has come for an era of integrated bridge system (IBS), an ECDIS was developed to receive more sensor information from a variety of navigational equipment.

Table 2. Type of sensors connected with an ECDIS

Type of Sensor	Received Information
Positioning System (GPS, GNSS)	Receives the ship's position signal
Gyro Compass	Receives ship's bearing information
Rate of Turn Indicator	Receives ship's heading and turning angle
Speed/Doppler log	Receives data on ship's maneuverability according to water depth, current and wind direction
Magnetic Compass	Receives magnetic bearing information
RADAR with ARPA	Prevents risk of collision by receiving radar and ARPA information
AIS	Receives direction and information of other ships
AutoPilot	Implementation of automatic ship steering control through ECDIS
Anemometer	Receives information for wind direction and speed
Echo Sounder	Receives information of water depth
NAVTEX	Receive navigation alerts, such as weather, casualty, and collisions.
Each Thermometer	Receive atmosphere and seawater temperature

3. Methodology

3.1 Survey Design

BIMCO divides cyber security into administrative and technical securities to protect information from cyber risks and includes the physical security as a part of the administrative security. In addition, 12 survey items were derived by referring to the results of KMI (2019), which presented four priorities for each item among the security risks presented in ISO/IEC 27001 (Table 3).

Table 3. ECDIS Vulnerability Improvement Factors Survey Topics

Security area		Contents
Administrative Security	(A1)	Raise awareness and train employees on how to protect information
	(A2)	Control the use of portable media (USB, portable PC etc)
	(A3)	Maintenance of S/W tools such as H/W, S/W upgrades and anti-virus (V3, etc.)
	(A4)	Establish emergency plans for cyber-attacks

Technical Security	(T1)	Restrict and control access to network ports, protocols, and services (such as login password settings)
	(T2)	Detect, block, and warn against cyber-attacks through the system
	(T3)	Control remote and wireless access by using encryption key (ex. WiFi)
	(T4)	Support data backup and recovery function
Physical Security	(P1)	Set physical security zone and control access
	(P2)	Ban on carrying out any equipment, information and software outside without prior approval
	(P3)	Ensure continuous availability (emergency power supply, etc.) and integrity (sensor connection, etc.) of equipment
	(P4)	Confirm removal of data and S/W license when discarding equipment including storage media

3.2 Importance–Performance Analysis (IPA)

IPA analysis compares and evaluates the association between the importance and performance of key attributes for analysis targets. (Martilla and James, 1977). Therefore, after the main attributes and factors of the analysis were determined, the data were collected through a survey, and a quadrant matrix was generated by using the collected data. The x-axis of the matrix represented the importance of the attribute, the y-axis represented the achievement of the attribute, and the average value of each attribute was plotted on the matrix. IPA analysis can also present policy priorities and implementation methods by raising the importance and performance of the matrix (Lim et al., 2017). The matrix is comprised of four quadrants with their own characteristics. The first quadrant reflected good work maintenance, which requires continuous management to maintain the current state. The second quadrant was the possible overkill, and good results were obtained if the over-invested resources were applied to the first or fourth quadrants. The third quadrant was a low priority section and did not require more investment than the current situation, and could be provided much later in the future. The fourth quadrant required the most concentrated effort and intensive investment because users were not satisfied with the current service.

However, traditional IPA assumes that importance and performance are independent; however, they are not. To compensate for this, Deng (2007) proposed converting the performance item for each attribute into a natural logarithm and by using the partial correlation coefficient derived through the partial correlation analysis with the overall performance as a relative importance value. The properties that belong to each domain of the modified IPA matrix were interpreted the same as the traditional IPA.

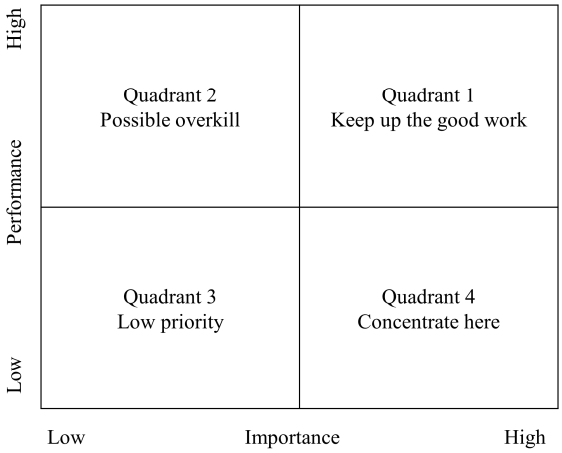

Fig. 1. The standard IPA chart.

For IPA analysis, a survey was conducted using a 5-point Likert scale for importance and performance of the items in Table 3 to ship operators who have used an ECDIS.

3.3 Reliability Analysis

The responses to the survey are presented on a 5-point Likert scale for importance and performance, and the Cronbach's alpha value was calculated using Equation (1) to verify the reliability of the survey response.

$$\alpha = \frac{k}{k-1}\left(1-\sum_{i=1}^{k}\frac{\sigma_i^2}{\sigma_t^2}\right) \quad \text{Equation (1)}$$

where, α: Value of Cronbach's alpha

k: Number of items

σ_i: Standard deviation of individual items

σ_t: Standard deviation of all items

4. Result & Discussion

4.1 Frequency Analysis

To evaluate ECDIS cyber security risk factors, a survey was conducted on officers who had experience using the ECDIS

onboard. Frequency analysis was conducted using 89 data points from a total of 100 (Table 5). The 2nd officers answered the most and questions followed by the 3rd officers. Most respondents had less than three years of onboard experience. As the ECDIS is navigation equipment that is mainly used by junior officers for voyage planning, the survey consisted of many answers from junior officers. The most used model was JRC. More than half (52.8%) of the respondents participated in cyber security-related training, and 22.5% of respondents had experience in ECDIS cyber-attacks.

Table 4. Characteristics of the survey sample (N = 89)

Characteristic		No. of respondents	Percentage (%)
Rank	Captain	11	12.4
	C/O	16	18.0
	2/O	31	34.8
	3/O	18	20.2
	etc	13	14.6
On board experience	0-3year	40	44.9
	3-5year	17	19.1
	> 5year	32	36.0
ECDIS model	JRC	46	51.7
	TRANSAS	2	2.2
	FURUNO	20	22.5
	MECys	19	21.3
	etc	2	2.2
Experience in education	Yes	47	52.8
	No	42	47.2
Experience in cyber-attack	Yes	20	22.5
	No	69	77.5

4.2 Reliability Analysis

The reliability assessment of survey items showed that both importance and performance have a Cronbach's alpha value of >0.9 and survey data are consistent (Cronbach, 1951).

Table 5. Result of reliability analysis

	Cronbach's alpha	Number of items
Importance	0.938	12
Performance	0.933	12

4.3 Independent Two Sample t-test

(1) Analysis results by the rank

An independent two-sample t-test was conducted to determine whether the importance and performance of ECDIS cyber security risk factors differed according to the officer's rank. The test results showed that, the importance of the senior group (M = 4.6) to the portable media control policy was significantly higher than that of the junior group (M = 4.041). In addition, for remote access control and wireless access (Wi-Fi, etc.) control using encryption keys, the junior group (M = 3.612) showed significantly higher achievement than the senior group (M = 3.154). In some items, there were significant differences between groups, however, there was no statistically significant difference between groups in terms of importance and achievement.

Table 6. T-test results by rank

Attribute	Importance			Performance		
	Average		p-value	Average		p-value
	Junior (49)	Senior (40)		Junior (49)	Senior (40)	
A1	4.163	4.250	.665	3.388	3.375	.951
A2	4.041	4.600	.008	3.653	3.725	.734
A3	4.122	4.275	.461	3.604	3.795	.387
A4	4.265	4.575	.102	3.653	3.525	.596
T1	4.184	4.400	.277	3.816	3.475	.097
T2	4.286	4.400	.581	3.510	3.282	.317
T3	4.143	4.205	.791	3.612	3.154	.045
T4	4.490	4.475	.939	4.000	3.825	.393
P1	4.224	4.375	.433	3.735	3.650	.707
P2	4.204	4.154	.510	3.714	3.325	.109
P3	4.204	4.077	.521	3.653	3.487	.427
P4	3.796	3.875	.747	3.571	3.500	.766

(2) Analysis results for cyber-attacks

An independent two-sample t-test was conducted to determine whether the importance and performance of the ECDIS cyber security risk factors differ according to the cyber-attack experience. The results showed that the attacked group (M = 4.05) had significantly higher achievement for establishing emergency plans for cyber-attacks than the group with no attack experience (M = 3.464). When experiencing a zero-cyber-attack, the plan that was established in advance during the course of action was helpful. There were significant differences between groups in some items; however, there was no statistically significant difference between the groups in terms of importance and performance.

Table 7. T-test results based on cyber-attack experience

Attribute	Importance			Performance		
	Average		p-value	Average		p-value
	Yes (20)	No (69)		Yes (20)	No (69)	
A1	4.200	4.203	.990	3.500	3.348	0.535
A2	4.300	4.290	.968	3.650	3.696	0.856
A3	4.300	4.159	.569	4.053	3.588	0.078
A4	4.500	4.377	.588	4.050	3.464	0.040
T1	4.100	4.333	.326	3.850	3.609	0.327
T2	4.300	4.348	.847	3.550	3.368	0.501
T3	3.750	4.232	.102	3.632	3.348	0.308
T4	4.550	4.464	.706	4.050	3.884	0.497
P1	4.200	4.319	.604	3.650	3.710	0.823
P2	4.050	4.159	.695	3.700	3.493	0.477
P3	4.200	4.072	.774	3.700	3.544	0.530
P4	3.550	3.913	.212	3.300	3.609	0.280

(3) Analysis results by completion of cyber security training

An independent two-sample t-test was conducted to determine whether the importance and performance of the ECDIS cyber security risk factors differ according to the completion of cyber security education. The results showed that test, there was no statistically significant difference between the groups in terms of importance and performance in all items.

Table 8. T-test result according to completion of cyber security training

Attribute	Importance			Performance		
	Average		p-value	Average		p-value
	Yes (47)	No (42)		Yes (47)	No (42)	
A1	4.191	4.214	.909	3.447	3.310	.504
A2	4.319	4.262	.790	3.787	3.571	.304
A3	4.255	4.119	.509	3.739	3.634	.633
A4	4.468	4.333	.478	3.745	3.429	.187
T1	4.149	4.429	.158	3.617	3.714	.638
T2	4.255	4.429	.401	3.391	3.429	.870
T3	4.043	4.317	.239	3.489	3.317	.454
T4	4.532	4.429	.589	4.043	3.786	.208
P1	4.319	4.262	.765	3.723	3.667	.801
P2	4.065	4.310	.154	3.638	3.429	.389
P3	4.170	4.122	.807	3.565	3.595	.885
P4	3.766	3.905	.569	3.596	3.476	.617

4.4 IPA Analysis

Since there was little significance in the average between groups based on the rank, cyber security training completion, and cyber-attack experience, IPA analysis was conducted on cyber security risk factors from the perspective of an officer who mainly uses the ECDIS. Fig. 2 shows the analysis results using traditional IPA. The first quadrant represents ‘keep up good work’ which indicates that officers believe that the properties of ‘data backup and recovery’, ‘secure zone control’, ‘portable media control’, ‘H/W and S/W upgrade’, ‘emergency plan establishment’, and ‘network access control’ are important and are being performed well. The third quadrant shows that ‘data and license disposal’, ‘guaranteed availability or integrity of equipment’, ‘ban on carrying out any information and software outside’, and ‘remote and wireless access control’ had the lowest priority. The fourth quadrant reflects ‘concentrate here’ and ‘raise awareness and train employees’ and ‘detect and block cyber-attacks’ were classified as the most urgently needed attributes.

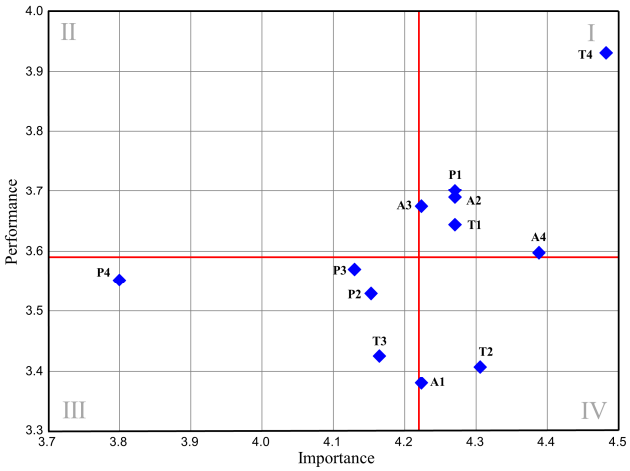

Fig. 2. Result of IPA analysis.

A modified IPA analysis was performed to supplement attributes that are skewed towards the first and third quadrants, which was highlighted as a persistent problem of traditional IPA by Deng (2007) (Fig. 3). Consequently, ‘portable media control’, ‘security zone control’ and ‘establish emergency plan’ were classified as performing well compared to their importance which was ‘possible overkill’. Furthermore, ‘guaranteed availability or integrity of equipment’, ‘detect and block cyber-attacks’, and ‘remote or wireless access control’ were classified as areas to be focused on.

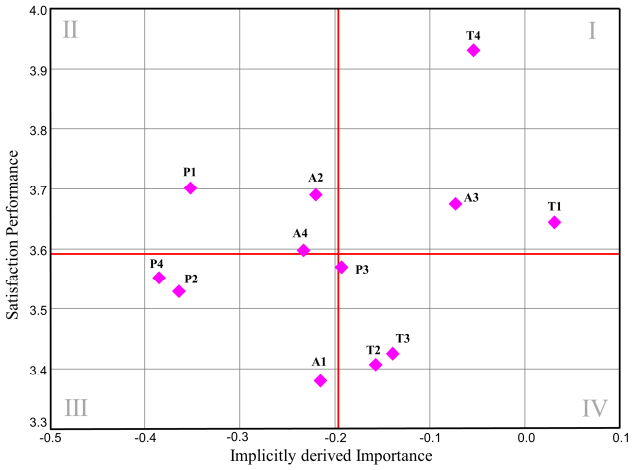

Fig. 3. Result of revised IPA analysis.

4.5 Discussion

The first hypothesis, “the level of performance or importance of current cyber security risk factors will differ depending on the officer’s rank, completion of cyber security training, and cyber-attack experience,” was rejected, except for some items. In other words, there was no difference in the average value of the survey according to the officer’s rank, cyber security training completion, and cyber-attack experience. Therefore, IPA analysis was conducted with officers who had actual ECDIS usage experience. IPA is a methodology mainly used to determine policy, however, since traditional methods have limitations, a modified IPA methodology was also used, and Table 9 shows the comparison of each result.

Table 9. Comparison of results of traditional IPA and modified IPA

Quadrant	IPA	Revised IPA
1 Quadrant	A2, **A3**, A4, **T1**, **T4**, P1	**A3, T1, T4**
2 Quadrant	-	A2, A4, P1
3 Quadrant	T3, **P2,** P3, **P4**	A1, **P2, P4**
4 Quadrant	A1, **T2**	**T2**, T3, P3

Policies that show the same results in both traditional and revised methodologies must be implemented first. 'H/W and S/W upgrade', 'network access control', and 'data backup and recovery' policies performed well in preventing cyber-attacks from an officer's perspective. Therefore, these policies should continue to be promoted in the future. However, it is necessary to postpone priorities and invest in other areas to address the items, namely, ‘ban on carrying out any information and software' and 'discard data and license'. Since the ECDIS is equipped with software and hardware on the bridge and operates continuously for 24h, it was found that there were limited opportunities for officers to remove the license during the voyage, which resulted in a low priority. 'detect and block cyber-attacks' was analyzed as the most urgent factor, which should be implemented.

This policy must be technically supported, and it was determined that technology development will be necessary to meet the needs of users and officers. According to a previous study, ‘detect and block cyber-attacks’ and ‘network access control’ had relatively high importance, and ‘removal of data and S/W license’ had the lowest importance (KMI, 2019). These findings were similar to the results obtained in this study based on the experience of ECDIS users. However, training was identified as an important item in previous studies, and it was not of high importance from the perspective of ECDIS users. This is so believed because the current official ECDIS training does not have any cyber security information; therefore, users do not perceive it to be significant (IMO, 2012).

5. Conclusion

The danger of cyber-attacks is increasing because of the rapid progress of digitalization. In particular, several cyber-attack that occurred in the maritime field proves that ships are targets for cyber-attacks. In particular, the ECDIS, which plays a key role in the transition from analog to digital navigation equipment, requires thorough preventive measures to prevent accidents. This study attempted to derive cyber security risk factors and examined the priorities of policies that must be implemented for officers using the ECDIS, which is the connection center for navigation devices. The conclusions drawn from this study are as follows :

(1) The ECDIS was connected to various navigational devices to display information, and needed periodic updates; therefore, external media were frequently connected and easily exposed to danger.

(2) Of all respondents, 52.8% completed cyber security training, and 22.5% had experience in cyber-attacks.

(3) There was no statistically significant difference between the importance and preference of cyber security risk factors by rank, completion of cyber security training, and cyber-attack

experience. In other words, the officer's idea of cyber security risks was independent of rank, training, and attack experience.

(4) According to the IPA analysis, 'cyber-attack detection and prevention' was analyzed as the priority, which is a technical measure and a factor that must be considered in future technology development. In addition, 'H/W and S/W upgrades', 'network access control', and 'data backup and recovery' were areas where current policies should be pursued.

This study derived cyber security risk factors and analyzed its priorities based on ECDIS users. However, the limitation of the study was that the analysis of maritime employees, and cyber security management policies was done on a small scale. In the future, such analysis should be conducted on a wide scale by expanding the scope to other industries.

Acknowledgement

This research was supported by the 'Development of Autonomous Ship Technology (20200615)' funded by the Ministry of Oceans and Fisheries (MOF, Korea).

References

[1] BIMCO(2018), The Guidelines on Cyber Security Onboard Ships, Ver. 3, pp. 10-11.

[2] Cronbach, L. J.(1951), Coefficient alpha and the internal structure of tests. Psychometrika, Vol. 16, No. 3, pp. 297-334.

[3] D'agostini, E. and S. H. Jo.(2019), Maritime Security Training: Evaluation of the Impact on Seafarers' Security Awareness and Security Performance, Journal of the Korean Society of Marine Environment & Safety, Vol. 25, No. 2, pp. 201-211.

[4] Deng, W.(2007), Using a revised importance performance analysis approach: The case of Taiwanese hot springs tourism, Tourism Management, Vol. 28, No. 5, pp. 1274-1284.

[5] IHO(2017), Information on IHO Standards related to ENC and ECDIS.Version 1.1. Monaco: IHO.

[6] IHO(2018), Current IHO ECDIS and ENC Standards. Monaco: IHO.

[7] IMO(2006), Resolution MSC.232(86), Adoption of the revised performance standard for Electronic Chart Display and Information System (ECDIS)

[8] IMO(2009a), Report of the Maritime Safety Committee on its Eighty-sixth Session, MSC 86/26, p. 13.

[9] IMO(2009b), Report of the Maritime Safety Committee on its Eighty-sixth Session, MSC 86/26/Add.1, Annex 1, pp. 3-4.

[10] IMO(2012), Operational use of electronic chart display and information systems (ECDIS) MODEL COURSE 1.27.

[11] IMO(2016), MSC 96th session, 11-20 May 2016, Cyber Security - interim guidelines approved.

[12] IMO(2017), Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems.

[13] Jung, M., Y. S. Park, and S. Y. Kang(2015), Analysis of User Requirement for the Improvement of ECDIS to Enhance Navigational Safety and Work Efficiency, Journal Korean Navigation and Port research, Vol. 39, No. 3, pp. 141-147.

[14] Kesseler, G. C.(2019), Cybersecurity in the Maritime Domain. USCG Proceedings of the Marine Safety & Security Council, 76(1). Retrieved from https://commons.erau.edu/publication/1318.

[15] KMI(2019), A Study on Strengthening Cybersecurity System in the Maritime Sector, Korea Maritiem Institute.

[16] Kwon, S. H., W. L. Jeong, and S. B. Moon(2021), A Relative Importance Evaluation of Bridge Navigational Equipment Using AHP, Journal Korean Navigation and Port research, Vol. 45, No. 1, pp. 9-15.

[17] Lee, B. K.(2018), Usability Test and Investigation of Improvements of the ECDIS, Journal of the Korean Society of Marine Environment & Safety, Vol. 24, No. 2, pp. 146-156.

[18] Lee, E. S., Y. J. Ahn, and S. H. Park(2020), A Study on the Development of a Training Course for Ship Cyber Security Officers, Journal of the Korean Society of Marine Environment & Safety, Vol. 26, No. 7, pp. 830-837.

[19] Lee, J. S., B. K. Lee, and I. S. Cho.(2019), Text Mining Analysis Technique on ECDIS Accident Report, Journal of the Korean Society of Marine Environment & Safety, Vol. 25, No. 4, pp. 405-412.

[20] Lim, S. G., S. C. So, and C. S. Lee(2017), An Empirical Analysis of the Performance of Goverment 3.0 'Service Goverment' Using IPA Analysis, Korean Journal of Public Administration, Vol. 55, No. 2, pp. 137-167.

[21] Martilla, J. A. and J. C. James(1977), Importance-Performance Analysis, Journal of Marketing, Vol. 41, No.3, pp. 77-79.

[22] OCIMF(2017), TMSA3 Fast Facts, p. 2.

[23] Svilicic, B. and B. David(2019), Raising Awareness on Cyber Security of ECDIS, TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 13, No. 1, pp. 231-236.

[24] Svilicic, B., K. Junzo, C. Jasmin, and B. Johan(2018), Assessing ship cyber risk: a framework and case study of ECDIS security, WMU Journal of Maritime Affairs, Vol. 18, pp. 509-520.

Received : 2021. 05. 06.
Revised : 2021. 05. 25.
Accepted : 2021. 05. 28.