2023 모의IMO총회
The 2023 Mock IMO Assembly

Suggestions for Developing Cyber Security Plan (CSP) Guidelines to Enhance Ship Cybersecurity

Team MASERA-T

CONTENTS

1 BACKGROUND

- Increased Ship's Digitalization
- Circumstances of Cyber Attack Risk

2 PROBLEM ANALYSIS

- Research Comparing Shipping Lines' CSP
- IMO Recommends CSP's Integration on SMS
- No guidance for CSP Development

3 SOLUTION

- Research Object ; Align with IMO SD
- Methodology & Results

4 CONCLUSION

- Summary & Contributions
- Limitations
- Final Remarks

1 BACKGROUND

- Increased Ship's Digitalization
- Circumstances of Cyber Attack Risk

3 SOLUTION

- Research Object ; Align with IMO SD
- Methodology & Results

PART 1

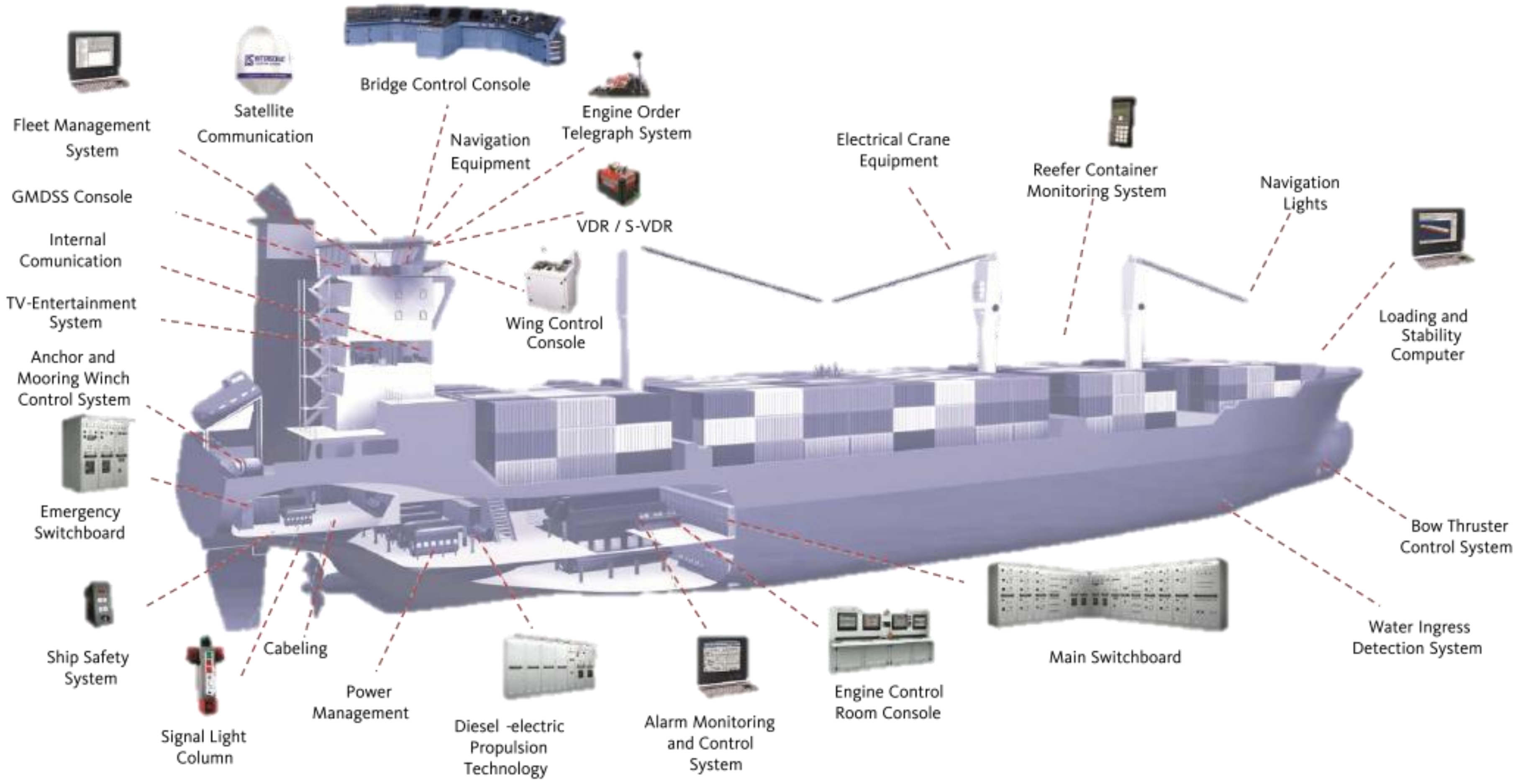
2 PROBLEM ANALYSIS

- Research Comparing Shipping Lines' CSP
- IMO Recommends CSP's Integration on SMS
- No guidance for CSP Development

4 CONCLUSION

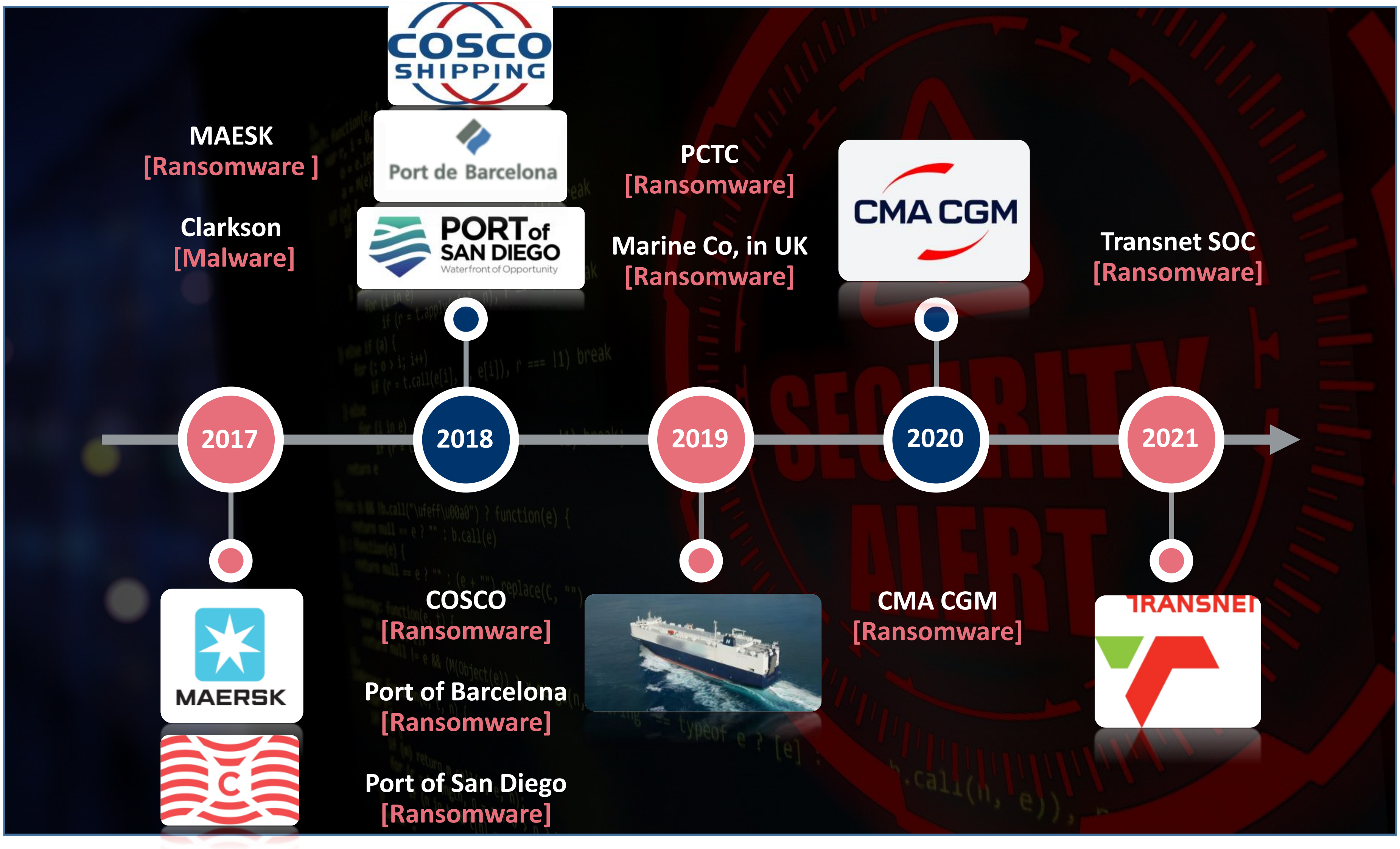
- Summary & Contributions
- Limitations
- Final Remarks

Increased Ship's Digitalization


Fleet Management System
Satellite Communication
Bridge Control Console
Engine Order Telegraph System
Navigation Equipment
GMDSS Console
Internal Comunication
TV-Entertainment System
Anchor and Mooring Winch Control System
Emergency Switchboard
VDR / S-VDR
Wing Control Console
Electrical Crane Equipment
Reefer Container Monitoring System
Navigation Lights
Loading and Stability Computer
Bow Thruster Control System
Water Ingress Detection System
Main Switchboard
Engine Control Room Console
Alarm Monitoring and Control System
Diesel -electric Propulsion Technology
Power Management
Cabeling
Signal Light Column
Ship Safety System

[1] The Picture of Ship Digitalization. Intercad.com

Circumstances of Cyber Attack Risk



2017

MAESK
[Ransomware]

Clarkson
[Malware]

2018

COSCO
[Ransomware]

Port of Barcelona
[Ransomware]

Port of San Diego
[Ransomware]

2019

PCTC
[Ransomware]

Marine Co, in UK
[Ransomware]

2020

CMA CGM
[Ransomware]

2021

Transnet SOC
[Ransomware]

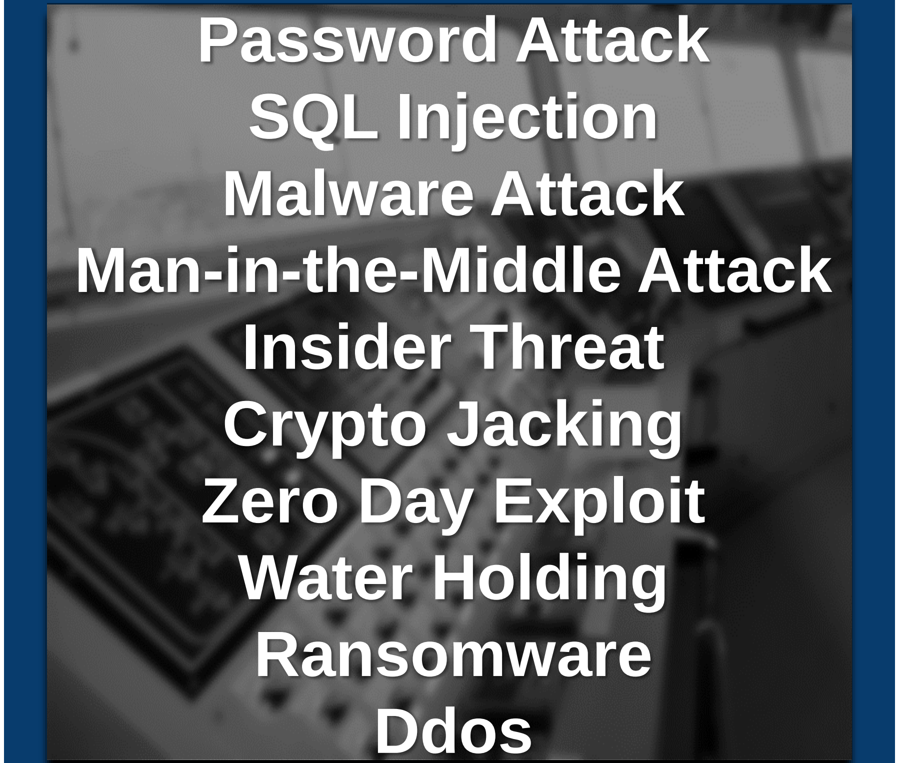
[2] Ref. Lim Junggyu et al. To establish cybersecurity trends and maritime cybersecurity, Technology Policy Proposal Research Collection, 2020

Circumstances of Cyber Attack Risk

GLOBAL MARITIME FORUM

The 2022 Global Maritime Issues Monitor Report Identifies ‘Maritime Cybersecurity’ as a Maritime Issue of Growing Importance in the Next Decade

Kinds of Cyber Security



Password Attack
SQL Injection
Malware Attack
Man-in-the-Middle Attack
Insider Threat
Crypto Jacking
Zero Day Exploit
Water Holding
Ransomware
Ddos

[3] Global Maritime Issues Monitor 2o22

PART 2

1 BACKGROUND

- Increased Ship's Digitalization
- Circumstances of Cyber Attack Risk

3 SOLUTION

- Research Object ; Align with IMO SD
- Methodology & Results

2 PROBLEM ANALYSIS

- Research Comparing Shipping Lines' CSP
- IMO Recommends CSP's Integration on SMS
- No guidance for CSP Development

4 CONCLUSION

- Summary & Contributions
- Limitations
- Final Remarks

Research comparing 8 Shipping Companies CSP

Lack of consistency in naming

Lack of visibility

Company	Cyber Security Plan's Name per Shipping Company	Remark
A	Cyber Security Instruction	Container shipping
B	Cyber Security Operation Guidance	Container shipping
C	Cyber Security Procedure	Bulk shipping
D	Cyber Security Response Plan	Tanker shipping
E	Cyber Security Procedure	Tanker shipping
F	Cyber Security Response Plan	Tanker shipping
G	Cyber Security Operation Guidance	Tanker shipping
H	Cyber Security Operation Guidance	Tanker Shipping

Research comparing 8 Shipping Companies CSP

	Contents	A	B	C	D	E	F	G	H
CRMA- 01	Identify Threats	X	O	O	O	O	O	O	O
CRMA-02	Identifying Vulnerabilities	O	O	X	O	O	O	O	X
CRMA-03	Risk Assessment	O	O	O	O	O	O	O	△
CRMA-04	Develop Protection and Detection Methods	△	△	O	O	△	O	△	△
CRMA-04	Create a Emergency Plan	O	△	△	O	O	△	O	O
CRMA-06	Security Incident Response and Recovery	O	△	X	△	O	△	O	O

BIMCO’s Cyber Security Guideline CRMA(Cyber Risk Management Approach)

O: Cites the guidelines and considers the characteristics of the breed.

△ : Cites the guidelines but does not reflect the characteristics of the breed or make any suggestions.

X: No citation of the guideline, no reflection of the breed, and no suggestions.

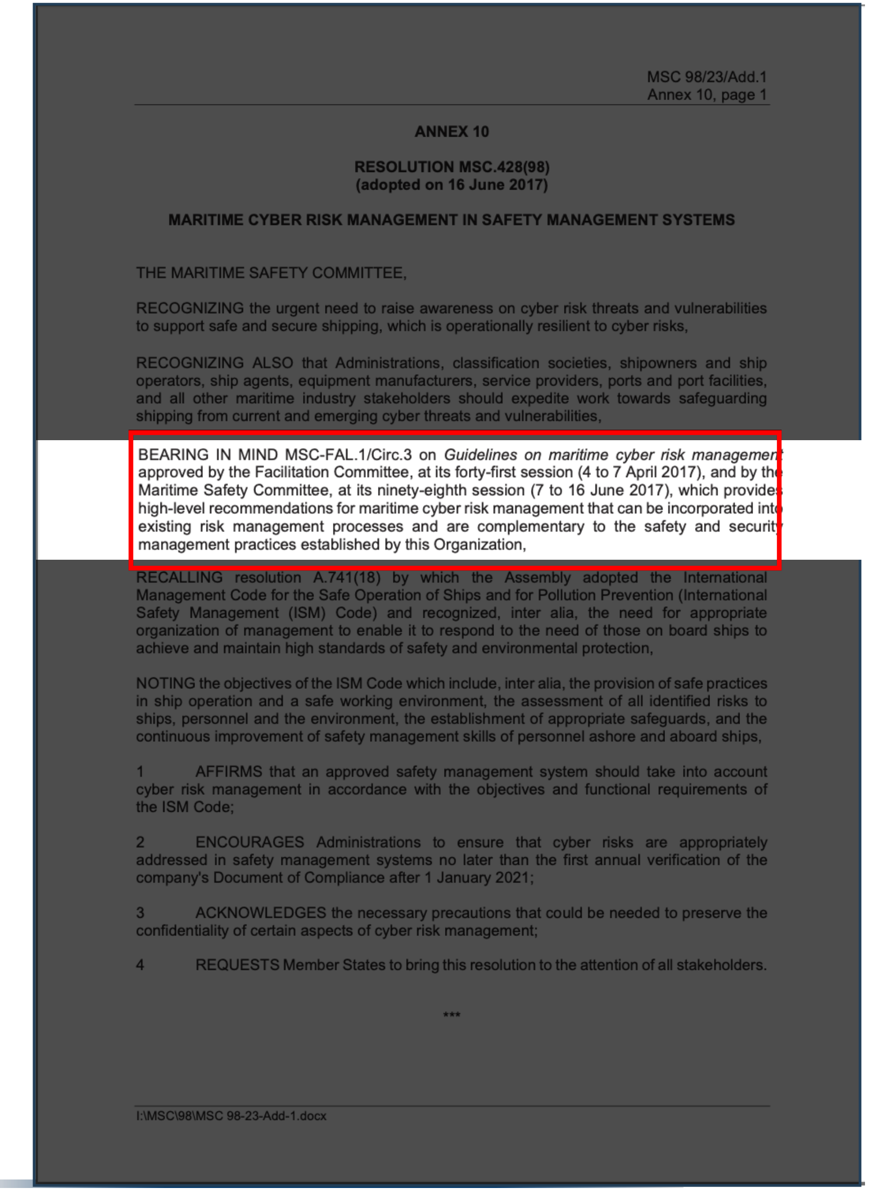
[4] Ahn, Y. J. and B. R. Kim, S. H. Park(2022), A study on comparison of ship cyber security plans and response systems, Journal of Navigation and Port Research, 2023 conference 2022.2: 396-397

Research comparing 8 Shipping Companies CSP

Differences in Including IMO Recommendations

Quality Differences between Shipping Lines

IMO recommends CSP's integration on SMS



MSC 98/23/Add.1
Annex 10, page 1

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

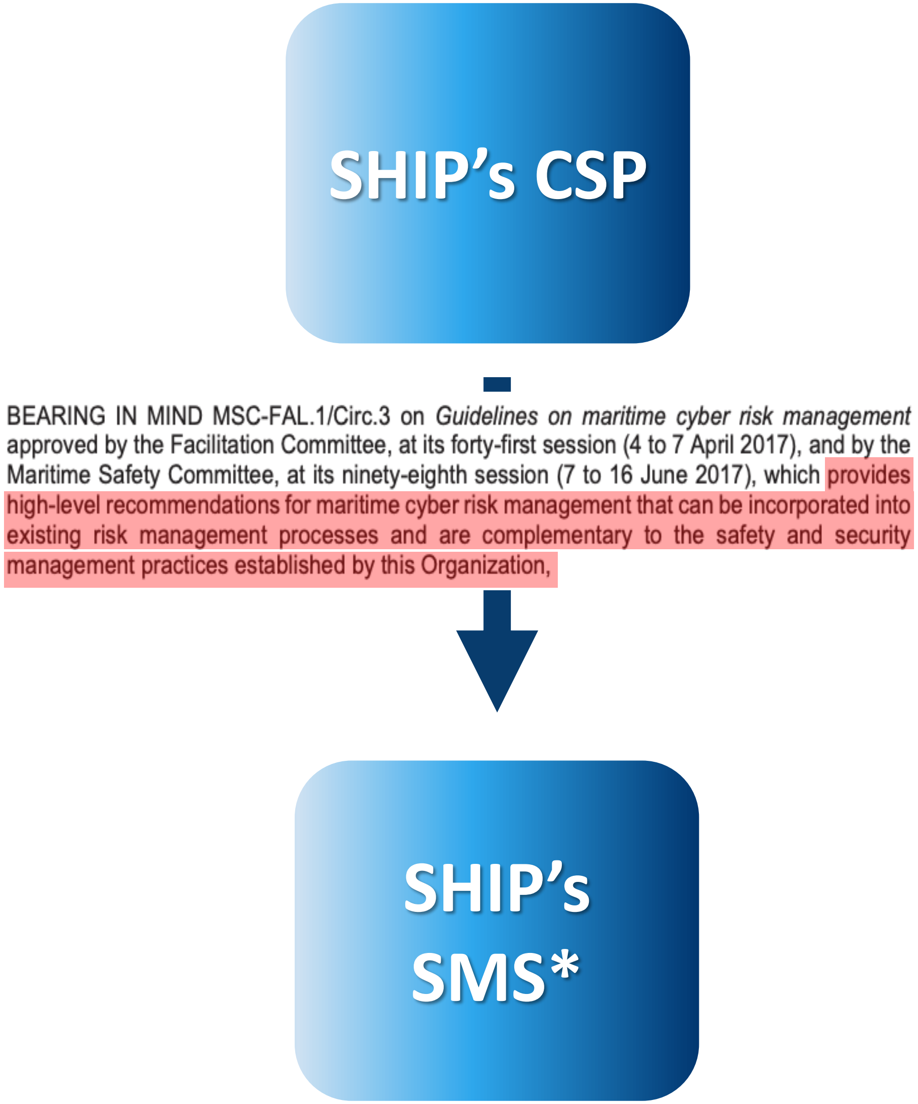
2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

I:\MSC\98\MSC 98-23-Add-1.docx



SHIP's CSP

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

SHIP's SMS*

[5] Resolution MSC.428(98) - <IMO Document>

SMS* : Ship Management System

No Guidance for CSP Development

BIMCO

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and suppo
BIMCO, CLIA, ICS, INTER

BIMCO CLIA
InterManager INTERTANKO

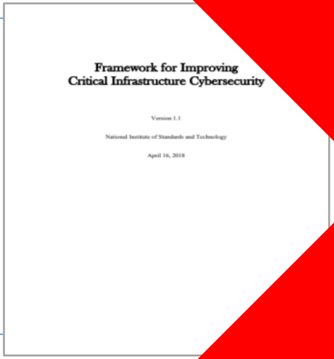
[1] Relationship to Stakeholders and Vulnerabilities

[2] Recognize Threats an isk Assessment

[3] Protection Action

[4] Emergency an e Plan

NIST



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

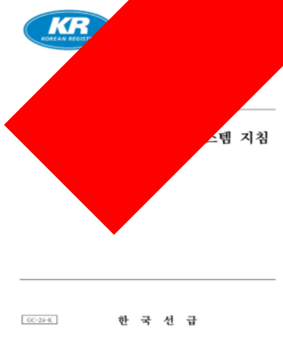
April 16, 2018

urity Framework Elements including

, Protecting, Responding and Recovering

the Framework Element

K R



KR
KOREAN REGIST

스템 지침

GC-24-K

한 국 선 급

[1] Identification tication of Data Confidentiality

[2] Data Confidentia

[3] Resource Availability

[4] Cybersecurity Requirements for Ship's System and Devices

[6] The Guidelines on Cybersecurity Onboard Ship - BIMCO
[7] Framework for Improving Critical Infrastructure Cybersecurity-NIST
[8] The Picture of 해상사이버보안가이드라인 - KR

1 BACKGROUND

- Increased Ship's Digitalization
- Circumstances of Cyber Attack Risk

3 SOLUTION

- Research Object ; Align with IMO SD
- Methodology & Results

PART 3

2 PROBLEM ANALYSIS

- Research Comparing Shipping Lines' CSP
- IMO Recommends CSP's Integration on SMS
- No guidance for CSP Development

4 CONCLUSION

- Summary & Contributions
- Limitations
- Final Remarks

Preface before Solution

There is no CSP Development Guideline In Any of the IMO Document

With Cybersecurity Threats on the Rise

Need to Create Efficient CSP Development Guidelines

Align with IMO's SD

2 Integrate new and advancing technologies in the regulatory framework

5 Enhance global facilitation and security of international trade

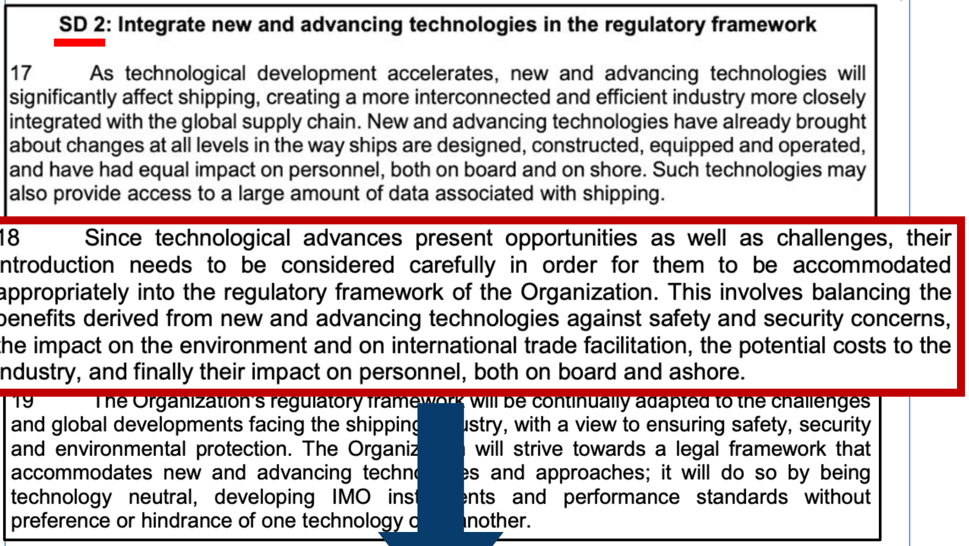
7 Ensure regulatory effectiveness

[9]Strategic Plan for the Organization for six- year period 2018 to 2023 (Resolution A .1110(30))

Align with IMO's SD

Strategic Plan for the Organization for 6 years Period 2018 to 2023 (Resolution A .1110(30))

MSC 107th Session 17.26 ~ 17.27

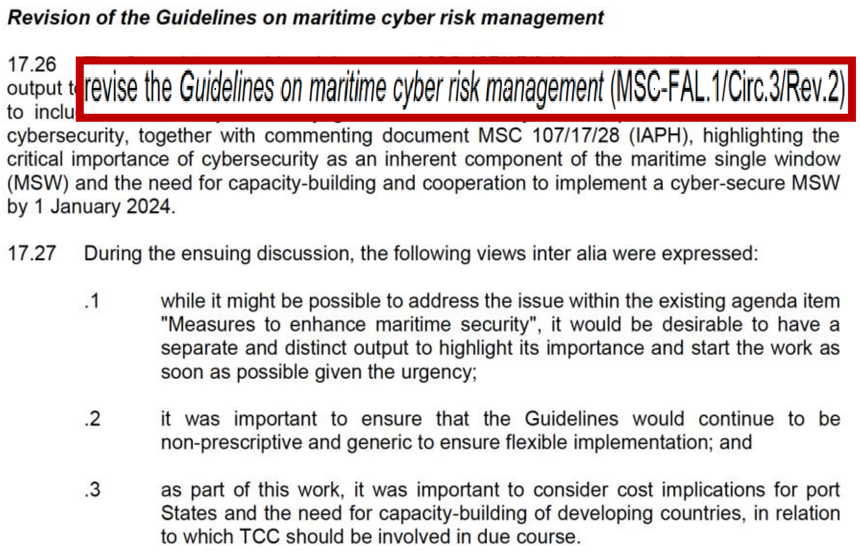


SD 2: Integrate new and advancing technologies in the regulatory framework

17 As technological development accelerates, new and advancing technologies will significantly affect shipping, creating a more interconnected and efficient industry more closely integrated with the global supply chain. New and advancing technologies have already brought about changes at all levels in the way ships are designed, constructed, equipped and operated, and have had equal impact on personnel, both on board and on shore. Such technologies may also provide access to a large amount of data associated with shipping.

18 Since technological advances present opportunities as well as challenges, their introduction needs to be considered carefully in order for them to be accommodated appropriately into the regulatory framework of the Organization. This involves balancing the benefits derived from new and advancing technologies against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry, and finally their impact on personnel, both on board and ashore.

19 The Organization's regulatory framework will be continually adapted to the challenges and global developments facing the shipping ustry, with a view to ensuring safety, security and environmental protection. The Organiz will strive towards a legal framework that accommodates new and advancing techn es and approaches; it will do so by being technology neutral, developing IMO inst ents and performance standards without preference or hindrance of one technology o nother.



Revision of the Guidelines on maritime cyber risk management

17.26 output t revise the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.2) to inclu cybersecurity, together with commenting document MSC 107/17/28 (IAPH), highlighting the critical importance of cybersecurity as an inherent component of the maritime single window (MSW) and the need for capacity-building and cooperation to implement a cyber-secure MSW by 1 January 2024.

17.27 During the ensuing discussion, the following views inter alia were expressed:

.1 while it might be possible to address the issue within the existing agenda item "Measures to enhance maritime security", it would be desirable to have a separate and distinct output to highlight its importance and start the work as soon as possible given the urgency;

.2 it was important to ensure that the Guidelines would continue to be non-prescriptive and generic to ensure flexible implementation; and

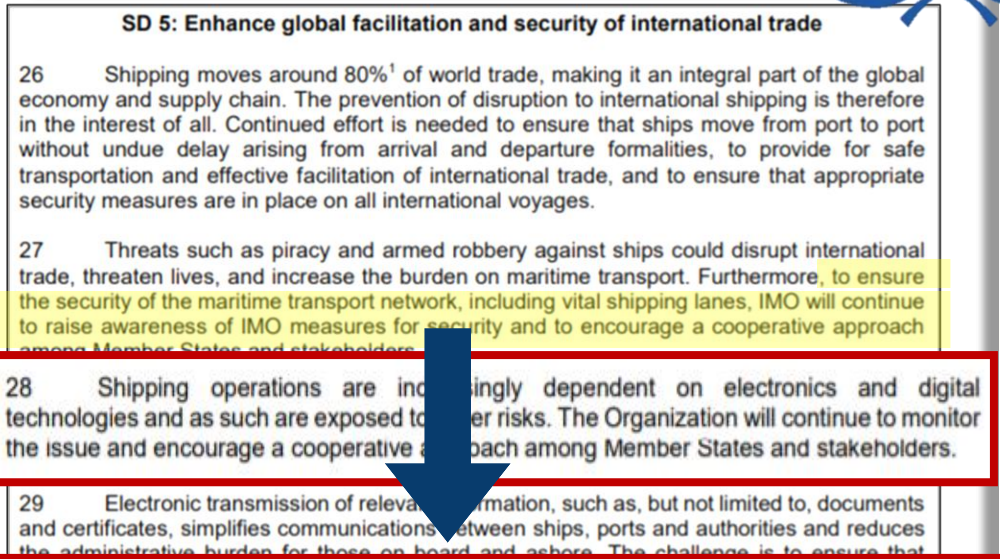
.3 as part of this work, it was important to consider cost implications for port States and the need for capacity-building of developing countries, in relation to which TCC should be involved in due course.

This involves balancing the benefits derived from new and advancing technologies against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry, and finally their impact on personnel, both on board and ashore.

[10] Strategic Plan for the Organization for six- year period 2018 to 2023 (Resolution A .1110(30))

Align with IMO's SD

Strategic Plan for the Organization for 6 years Period 2018 to 2023 (Resolution A .1110(30))



SD 5: Enhance global facilitation and security of international trade

26 Shipping moves around 80%[1] of world trade, making it an integral part of the global economy and supply chain. The prevention of disruption to international shipping is therefore in the interest of all. Continued effort is needed to ensure that ships move from port to port without undue delay arising from arrival and departure formalities, to provide for safe transportation and effective facilitation of international trade, and to ensure that appropriate security measures are in place on all international voyages.

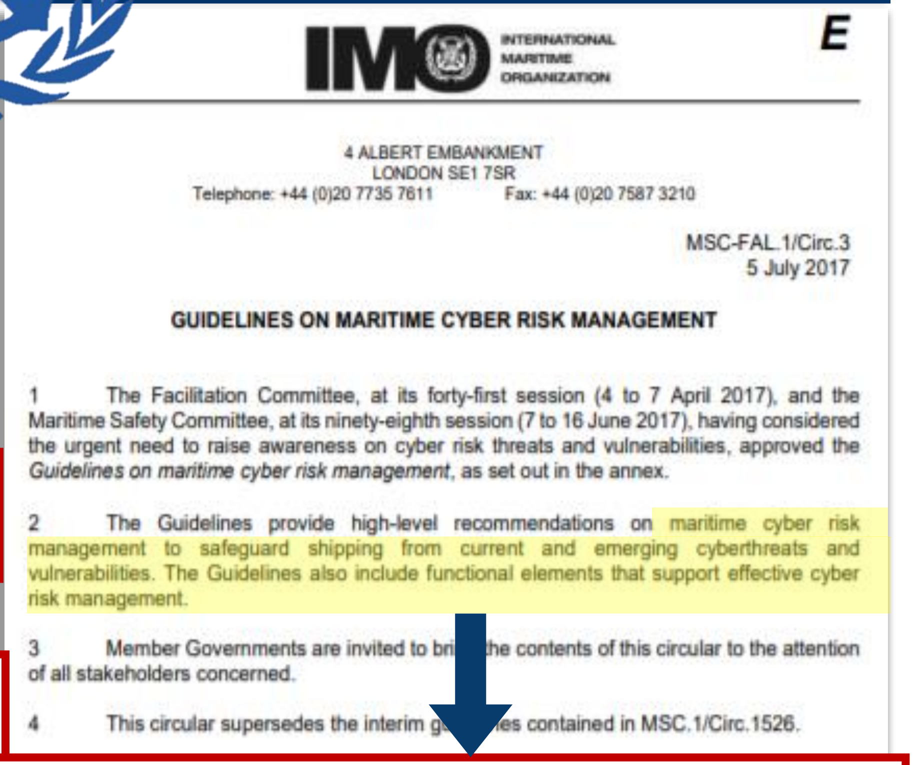
27 Threats such as piracy and armed robbery against ships could disrupt international trade, threaten lives, and increase the burden on maritime transport. Furthermore, to ensure the security of the maritime transport network, including vital shipping lanes, IMO will continue to raise awareness of IMO measures for security and to encourage a cooperative approach among Member States and stakeholders.

28 Shipping operations are increasingly dependent on electronics and digital technologies and as such are exposed to cyber risks. The Organization will continue to monitor the issue and encourage a cooperative approach among Member States and stakeholders.

29 Electronic transmission of relevant information, such as, but not limited to, documents and certificates, simplifies communications between ships, ports and authorities and reduces the administrative burden for those on board and ashore. The challenge is to ensure that

to ensure the security of the maritime transport network, including vital shipping lanes, IMO will continue to raise awareness of IMO measures for security and to encourage a cooperative approach among Member States and stakeholders.

Guidelines on Maritime Cyber Risk Management



IMO INTERNATIONAL MARITIME ORGANIZATION E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

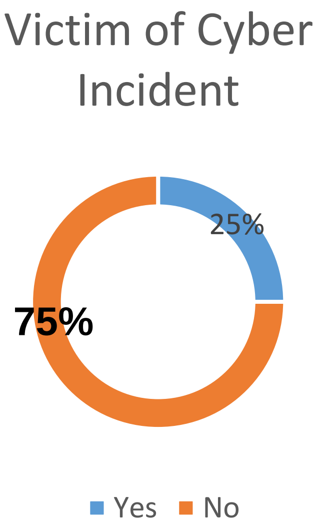
3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

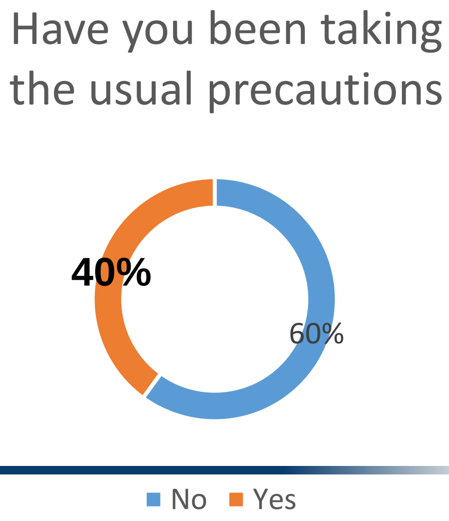
4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

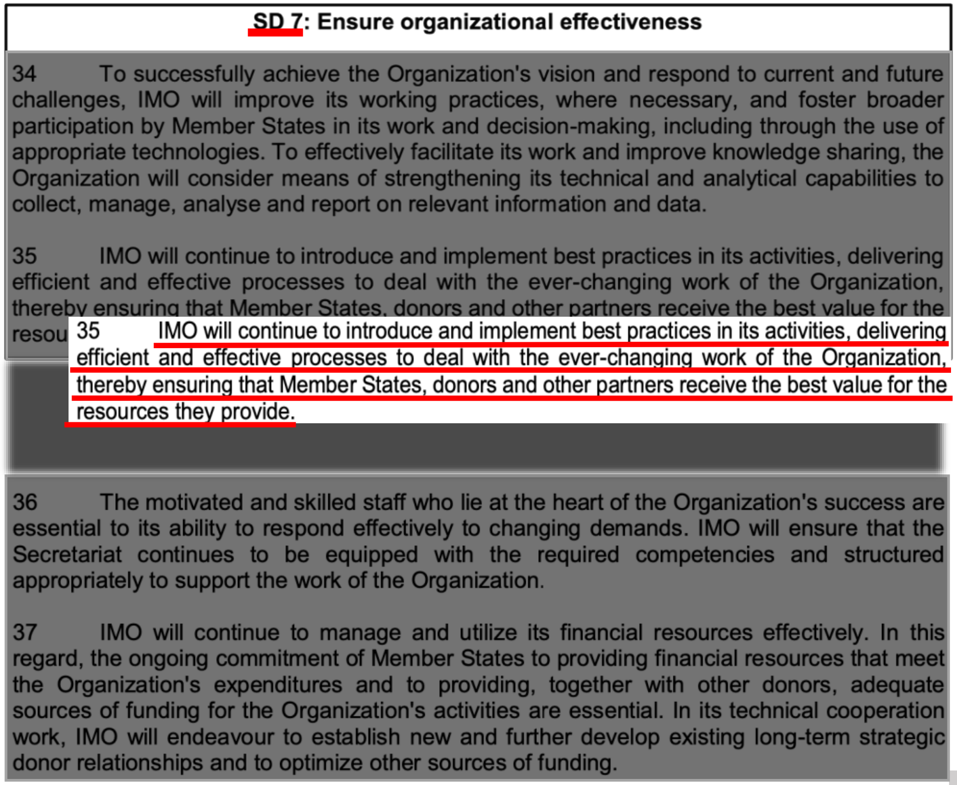
Align with IMO's SD

2016 BIMCO Cyber Threat Survey





Strategic Plan for the Organization for six- year period 2018 to 2023 (Resolution A .1110(30))



SD 7: Ensure organizational effectiveness

34 To successfully achieve the Organization's vision and respond to current and future challenges, IMO will improve its working practices, where necessary, and foster broader participation by Member States in its work and decision-making, including through the use of appropriate technologies. To effectively facilitate its work and improve knowledge sharing, the Organization will consider means of strengthening its technical and analytical capabilities to collect, manage, analyse and report on relevant information and data.

35 IMO will continue to introduce and implement best practices in its activities, delivering efficient and effective processes to deal with the ever-changing work of the Organization, thereby ensuring that Member States, donors and other partners receive the best value for the resou

35 IMO will continue to introduce and implement best practices in its activities, delivering efficient and effective processes to deal with the ever-changing work of the Organization, thereby ensuring that Member States, donors and other partners receive the best value for the resources they provide.

36 The motivated and skilled staff who lie at the heart of the Organization's success are essential to its ability to respond effectively to changing demands. IMO will ensure that the Secretariat continues to be equipped with the required competencies and structured appropriately to support the work of the Organization.

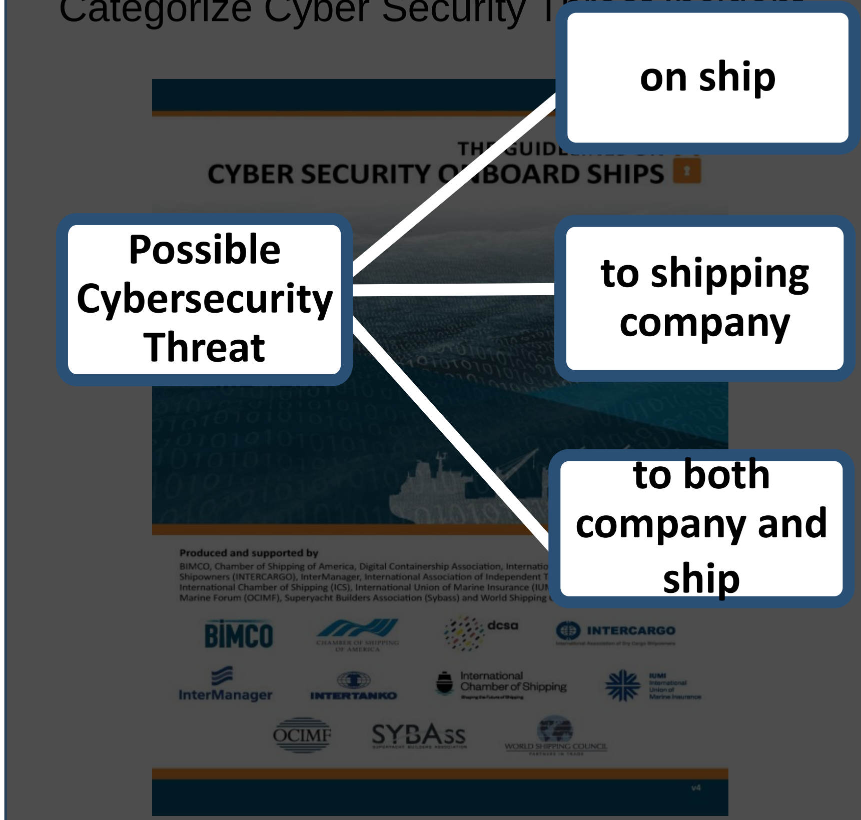
37 IMO will continue to manage and utilize its financial resources effectively. In this regard, the ongoing commitment of Member States to providing financial resources that meet the Organization's expenditures and to providing, together with other donors, adequate sources of funding for the Organization's activities are essential. In its technical cooperation work, IMO will endeavour to establish new and further develop existing long-term strategic donor relationships and to optimize other sources of funding.

Methodology & Results

Content Analysis BIMCO Guideline

Instrumental Analysis Resolution MEPC.54(32)

Categorize Cyber Security Threat Incident



Possible Cybersecurity Threat

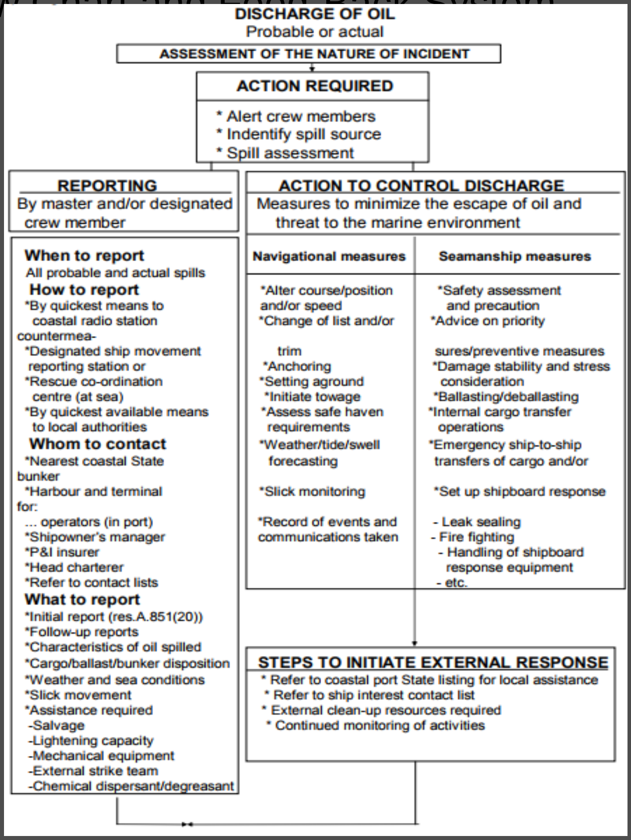
on ship

to shipping company

to both company and ship

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS
Produced and supported by
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)
BIMCO
CHAMBER OF SHIPPING OF AMERICA
dcsa
INTERCARGO
InterManager
INTERTANKO
International Chamber of Shipping
IUMI
OCIMF
SYBAss
WORLD SHIPPING COUNCIL
v4

Flow Chart and Feed Back System



DISCHARGE OF OIL
Probable or actual

ASSESSMENT OF THE NATURE OF INCIDENT

ACTION REQUIRED

* Alert crew members
* Indentify spill source
* Spill assessment

REPORTING
By master and/or designated crew member

When to report
All probable and actual spills

How to report
*By quickest means to coastal radio station
*Designated ship movement reporting station or
*Rescue co-ordination centre (at sea)
*By quickest available means to local authorities

Whom to contact
*Nearest coastal State
*Harbour and terminal
... operators (in port)
*Shipowner's manager
*P&I insurer
*Head charterer
*Refer to contact lists

What to report
*Initial report (res.A.851(20))
*Follow-up reports
*Characteristics of oil spilled
*Cargo/ballast/bunker disposition
*Weather and sea conditions
*Slick movement
*Assistance required
-Salvage
-Lightening capacity
-Mechanical equipment
-External strike team
-Chemical dispersant/degreasant

ACTION TO CONTROL DISCHARGE
Measures to minimize the escape of oil and threat to the marine environment

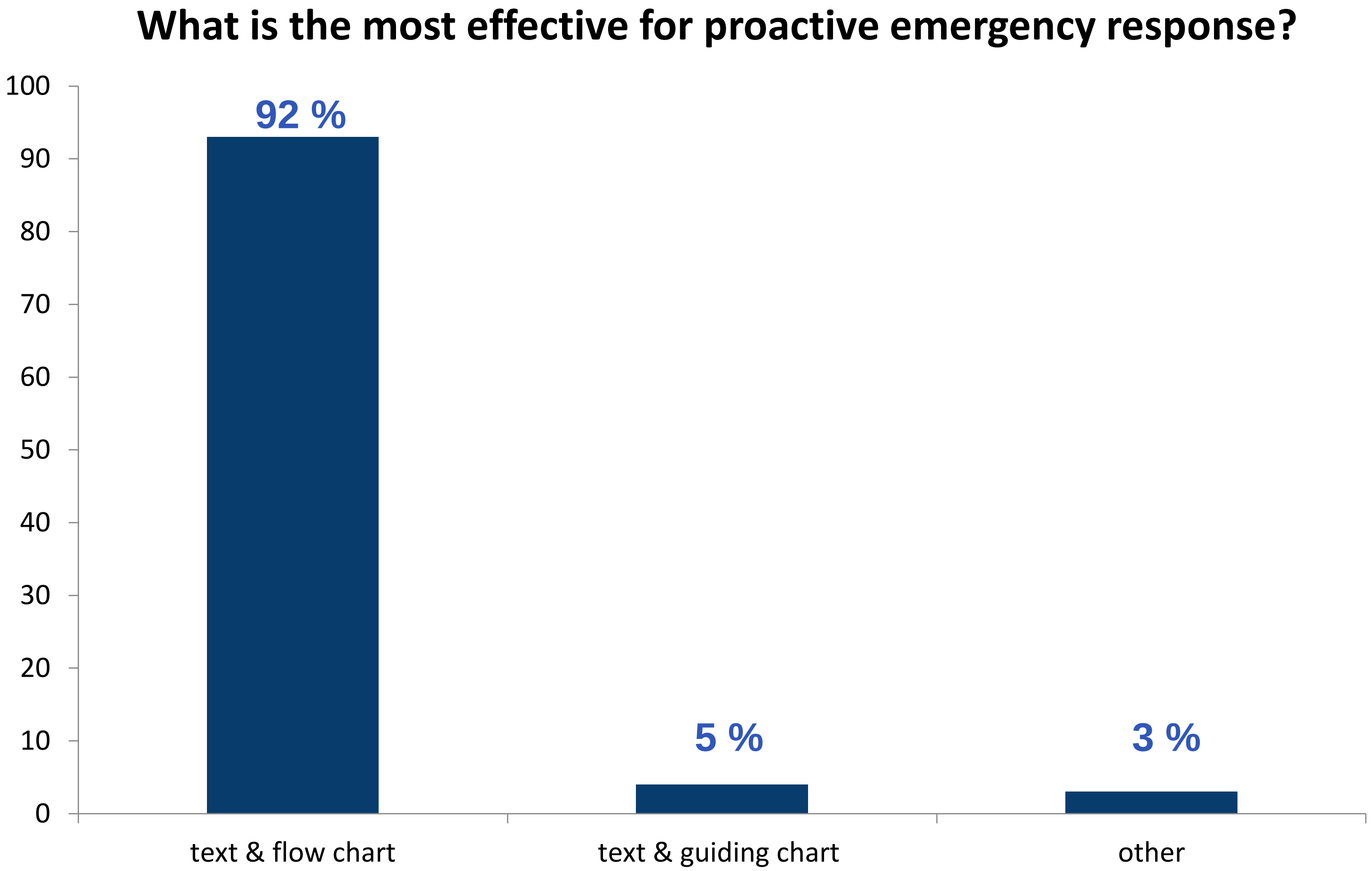
Navigational measures
*Alter course/position and/or speed
*Change of list and/or trim
*Anchoring
*Setting aground
*Initiate towage
*Assess safe haven requirements
*Weather/tide/swell forecasting
*Slick monitoring
*Record of events and communications taken

Seamanship measures
*Safety assessment and precaution
*Advice on priority countermeasures/preventive measures
*Damage stability and stress consideration
*Ballasting/deballasting
*Internal cargo transfer operations
*Emergency ship-to-ship transfers of cargo and/or bunker
*Set up shipboard response for:
- Leak sealing
- Fire fighting
- Handling of shipboard response equipment
- etc.

STEPS TO INITIATE EXTERNAL RESPONSE
* Refer to coastal port State listing for local assistance
* Refer to ship interest contact list
* External clean-up resources required
* Continued monitoring of activities

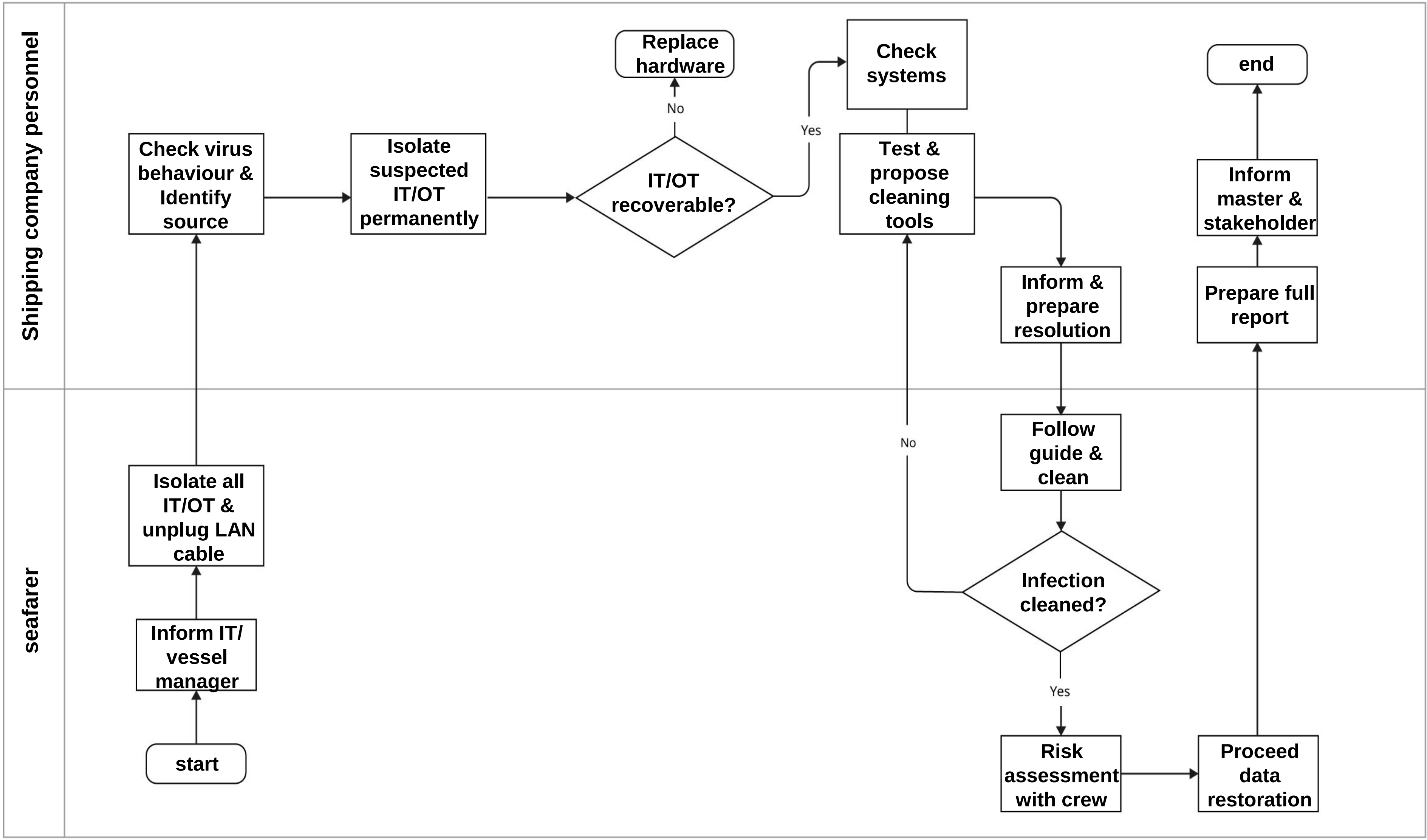
[11] Shipboard Oil Pollution Emergency Plans (Resolution MEPC.54(32)

Methodology & Results



Methodology & Results

Flowchart example when ship is infected by malware or ransomware


Shipping company personnel
seafarer
start
Inform IT/ vessel manager
Isolate all IT/OT & unplug LAN cable
Check virus behaviour & Identify source
Isolate suspected IT/OT permanently
IT/OT recoverable?
No
Replace hardware
Yes
Check systems
Test & propose cleaning tools
Inform & prepare resolution
Follow guide & clean
Infection cleaned?
No
Yes
Risk assessment with crew
Proceed data restoration
Prepare full report
Inform master & stakeholder
end

PART 4

1 BACKGROUND

- Increased Ship's Digitalization
- Circumstances of Cyber Attack Risk

2 PROBLEM ANALYSIS

- Research Comparing Shipping Lines' CSP
- IMO Recommends CSP's Integration on SMS
- No guidance for CSP Development

3 SOLUTION

- Research Object ; Align with IMO SD
- Methodology & Results

4 CONCLUSION

- Summary & Contributions
- Limitations
- Final Remarks

Summary

Instrumental Analysis

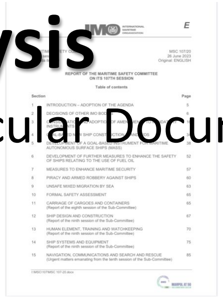
By utilizing the form of SOPEP

→ Instrumental Guideline

Contents Analysis

By referring to IMO Circular Documents and BIMCO's Guidelines

→ Contents Guideline



IMO INTERNATIONAL MARITIME ORGANIZATION E

MSC 107/20
26 June 2023
Original: ENGLISH

REPORT OF THE MARITIME SAFETY COMMITTEE ON ITS 107TH SESSION

Table of contents

I:\MSC\107\MSC 107-20.docx

MARPOL AT 50

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by

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)

→

CSP Production Guidelines

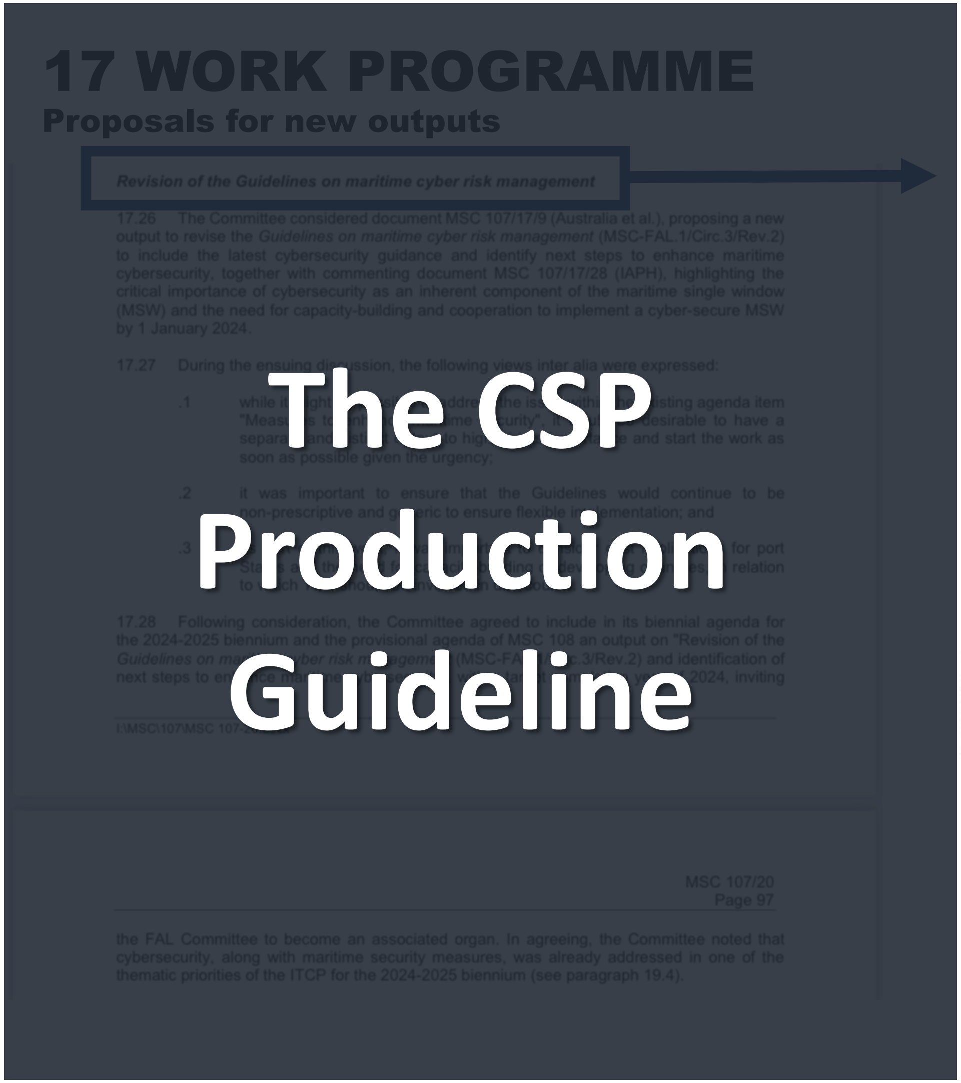
Opinions Of Stakeholders

Based on Research Findings and Opinions from Stakeholders

→ Making a Basic Foundation of CSP

[12] The Picture of SOPEP. mdnautical.com
[13] IMO MSC 107/20
[14] The Picture of Guideline from BIMCO The Guidelines on Cybersecurity Onboard Ship

Contributions



The CSP Production Guideline

17 WORK PROGRAMME

Proposals for new outputs

Revision of the Guidelines on maritime cyber risk management

17.26 The Committee considered document MSC 107/17/9 (Australia et al.), proposing a new output to revise the *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.2) to include the latest cybersecurity guidance and identify next steps to enhance maritime cybersecurity, together with commenting document MSC 107/17/28 (IAPH), highlighting the critical importance of cybersecurity as an inherent component of the maritime single window (MSW) and the need for capacity-building and cooperation to implement a cyber-secure MSW by 1 January 2024.

17.27 During the ensuing discussion, the following views inter alia were expressed:

.1 while it [illegible] address the issue within the existing agenda item "Measures to enhance maritime security", it [illegible] desirable to have a separate and distinct [illegible] to high[illegible] and start the work as soon as possible given the urgency;

.2 it was important to ensure that the Guidelines would continue to be non-prescriptive and generic to ensure flexible implementation; and

.3 [illegible] for port States [illegible] relation to which [illegible]

17.28 Following consideration, the Committee agreed to include in its biennial agenda for the 2024-2025 biennium and the provisional agenda of MSC 108 an output on "Revision of the *Guidelines on ma[illegible]ber risk management*" (MSC-FA[illegible]c.3/Rev.2) and identification of next steps to en[illegible] 2024, inviting

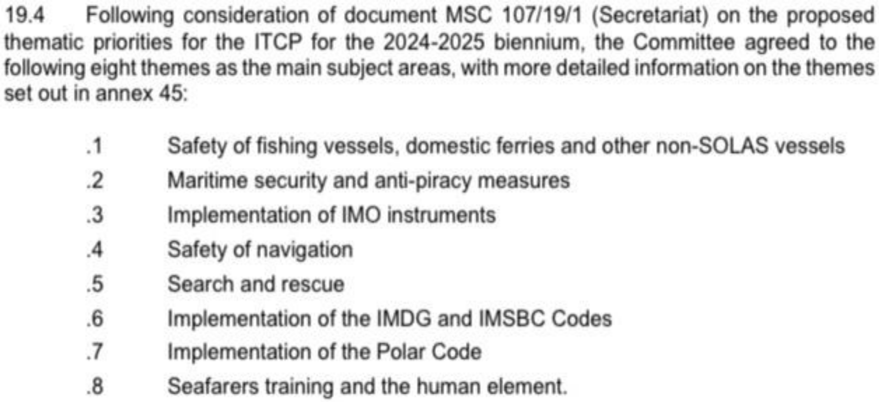
I:\MSC\107\MSC 107-2[illegible]

MSC 107/20
Page 97

the FAL Committee to become an associated organ. In agreeing, the Committee noted that cybersecurity, along with maritime security measures, was already addressed in one of the thematic priorities of the ITCP for the 2024-2025 biennium (see paragraph 19.4).

Revision of the Guidelines on Maritime Cyber Risk Management

MSC.108



19.4 Following consideration of document MSC 107/19/1 (Secretariat) on the proposed thematic priorities for the ITCP for the 2024-2025 biennium, the Committee agreed to the following eight themes as the main subject areas, with more detailed information on the themes set out in annex 45:

.1 Safety of fishing vessels, domestic ferries and other non-SOLAS vessels
.2 Maritime security and anti-piracy measures
.3 Implementation of IMO instruments
.4 Safety of navigation
.5 Search and rescue
.6 Implementation of the IMDG and IMSBC Codes
.7 Implementation of the Polar Code
.8 Seafarers training and the human element.

Limitations

Absence of All Current & Evolving Cybersecurity Issue

Year	Sector	System	Security	Details
2017	Maersk	Terminal IT System	Ransomware	System was paralyzed for 3weeks, 3,000 hundred million loss
2017	Containership	Navigation System in Ship	Mal-Ware	Loss of control for 10 hours
2017	Clarkson	Co, IT System	Insider	Trial to flow out company data
2018	Maritime Co,	Co, E-Mail	Spear Fishing	Loss at least 100 hundred million per year
2018	COSCO Shipping	IT System	Ransomware	Delayed transportation
2018	Barcelona Port	Port IT System	Ransomware	System closed & Request forensic
2018	San Diego Port	Port IT System	Ransomware	System closed & Request forensic
2019	PCTC	Ship IT System	Ransomware	Format the system
2019	Marine Co, in UK	Co, IT System	Ransomware	Fall in stock prices, request forensic
2020	CMA CGM	Co, IT System	Ransomware	Down the network systems for 2 weeks
2021	Transnet SOC	Port IT System	Ransomware	Knock-down all port terminal

[15] Ref. Lim Junggyu et al. To establish cybersecurity trends and maritime cybersecurity, Technology Policy Proposal Research Collection, 2020

Limitations

Limited Research Documents

IMO INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
107th session
Agenda item 20

MSC 107/20
26 June 2023
Original: ENGLISH

**REPORT OF THE MARITIME SAFETY COMMITTEE
ON ITS 107TH SESSION**

Table of contents

I:\MSC\107\MSC 107-20.docx

MARPOL AT 50

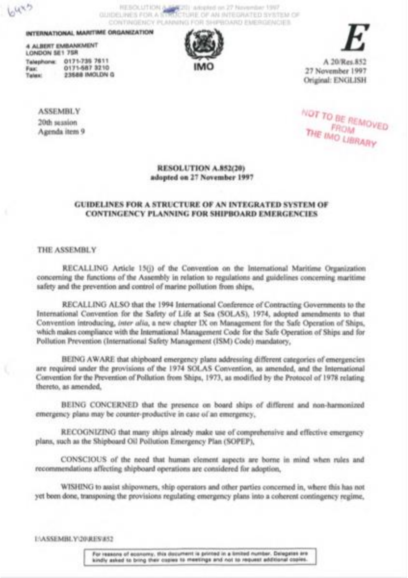
IMO Documents

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
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)

BIMCO
CHAMBER OF SHIPPING OF AMERICA
dcsa
INTERCARGO
InterManager
INTERTANKO
International Chamber of Shipping
IUMI International Union of Marine Insurance
OCIMF
SYBAss
WORLD SHIPPING COUNCIL
v4

BIMCO Guideline



64x5

RESOLUTION A.[illegible](20) adopted on 27 November 1997
GUIDELINES FOR A STRUCTURE OF AN INTEGRATED SYSTEM OF
CONTINGENCY PLANNING FOR SHIPBOARD EMERGENCIES

INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: 0171-735 7611
Fax: 0171-587 3210
Telex: 23588 IMOLDN G

IMO

E

A 20/Res.852
27 November 1997
Original: ENGLISH

ASSEMBLY
20th session
Agenda item 9

**RESOLUTION A.852(20)
adopted on 27 November 1997**

**GUIDELINES FOR A STRUCTURE OF AN INTEGRATED SYSTEM OF
CONTINGENCY PLANNING FOR SHIPBOARD EMERGENCIES**

THE ASSEMBLY

RECALLING Article 15(j) of the Convention on the International Maritime Organization concerning the functions of the Assembly in relation to regulations and guidelines concerning maritime safety and the prevention and control of marine pollution from ships,

RECALLING ALSO that the 1994 International Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, adopted amendments to that Convention introducing, *inter alia*, a new chapter IX on Management for the Safe Operation of Ships, which makes compliance with the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) mandatory,

BEING AWARE that shipboard emergency plans addressing different categories of emergencies are required under the provisions of the 1974 SOLAS Convention, as amended, and the International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto, as amended,

BEING CONCERNED that the presence on board ships of different and non-harmonized emergency plans may be counter-productive in case of an emergency,

RECOGNIZING that many ships already make use of comprehensive and effective emergency plans, such as the Shipboard Oil Pollution Emergency Plan (SOPEP),

CONSCIOUS of the need that human element aspects are borne in mind when rules and recommendations affecting shipboard operations are considered for adoption,

WISHING to assist shipowners, ship operators and other parties concerned in, where this has not yet been done, transposing the provisions regulating emergency plans into a coherent contingency regime,

I:\ASSEMBLY\20\RES\852

For reasons of economy, this document is printed in a limited number. Delegates are kindly asked to bring their copies to meetings and not to request additional copies.

SOPEP

Need for Diversifying the Kind of Research Documents

Limitations

Lack of Input from Other Countries

Differences in ***Awareness*** of Cybersecurity by country

Differences in the ***Level*** of Cybersecurity by Country

Differences in ***Infrastructure*** across country for Cybersecurity

[16] The Picture of IMO. Voakorea.com

Limitations

Constraints Scope of Survey

Limited Officers

	Contents	A	B	C	D	E	F	G	H
CRMA-01	Identify Threats	X	O	O	O	O	O	O	O
CRMA-02	Identifying Vulnerabilities	O	O	X	O	O	O	O	X
CRMA-03	Risk Assessment	O	O	O	O	O	O	O	△
CRMA-04	Develop Protection and Detection Methods	△	△	O	O	△	O	△	△
CRMA-04	Create a Emergency Plan	O	△	△	O	O	△	O	O
CRMA-06	Security Incident Response and Recovery	O	△	X	△	O	△	O	O

8 Shipping Companies only from Korea

Final Remarks

SHORT TERM

Increased Adoption of guideline for CSP

MIDDLE TERM

Achieve the Unity of CSP

LONG TERM

Safeguard the Maritime Industry

Ensure safe , Secure and Efficient Shipping on Clean Oceans

2023 모의IMO총회
The 2023 Mock IMO Assembly

THANK YOU

Team MASERA-T