Cybersecurity for ports: new challenges and solutions

IAPH Cybersecurity Guidelines for Ports:

iaph
international association
of ports and harbors

Gadi Benmoshe,
Vice-Chair IAPH DCC, Managing Director, Marinnovators

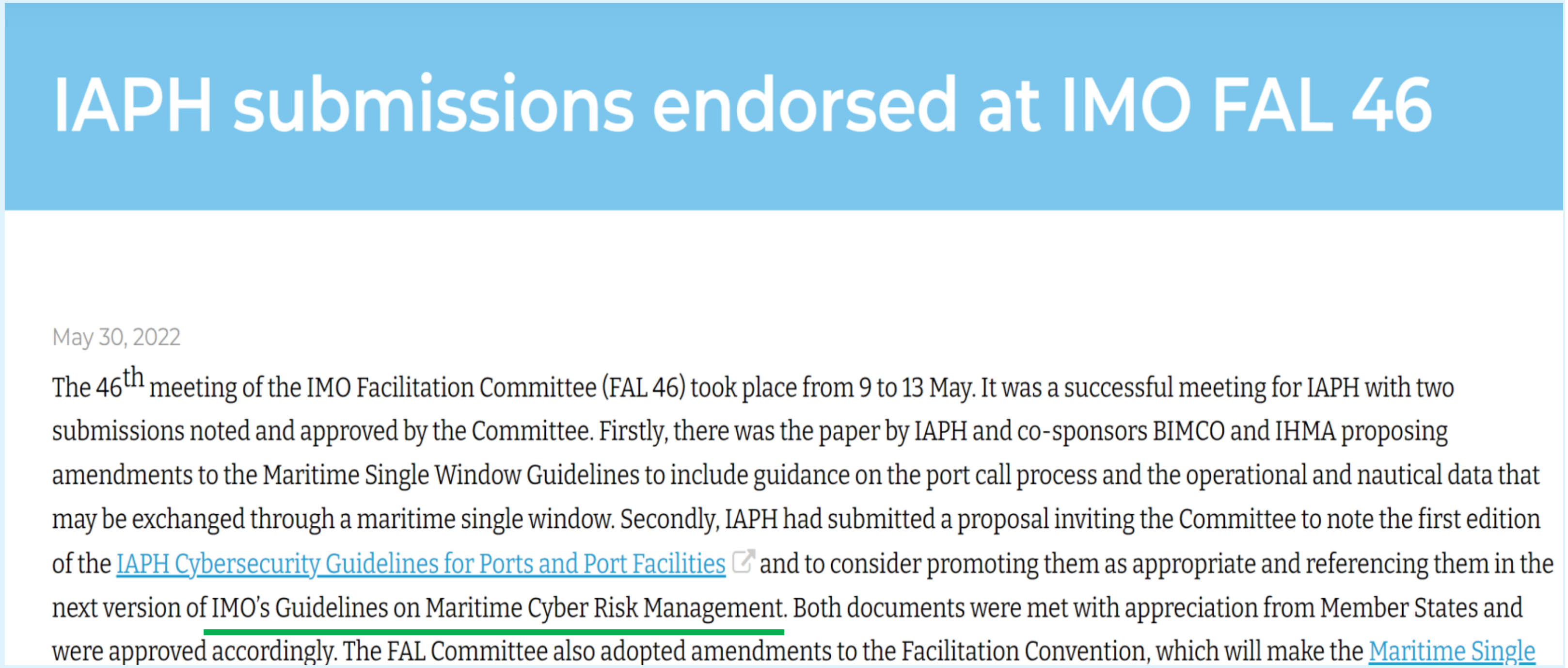
**'Decarbonization and Digitalization of Ports and Freight Transport:
The Contribution of EU Territorial Cooperation'
21/6/23**

Marinnovators
Consulting Services: Digital Transformation, Innovation, Cybersecurity

What are the guidelines?

This **84 page** document is the culmination of **four months** of intense work between **22 experts** from IAPH member ports from around the world as well as Associate Member cybersecurity specialists and contributors from the World Bank.

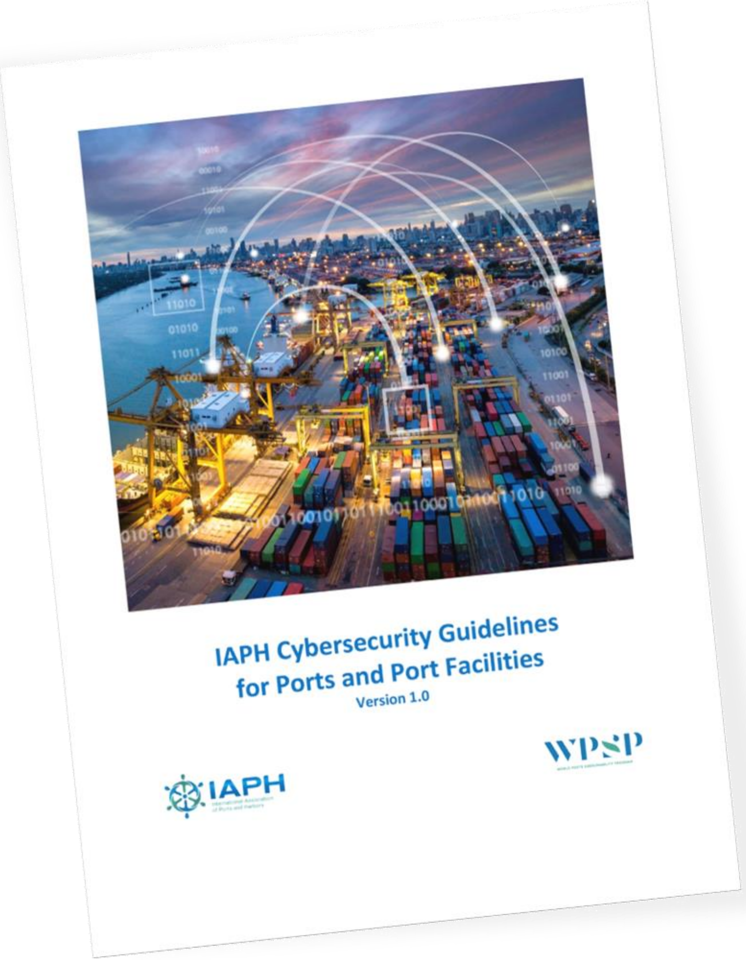
Its purpose is to serve as a **crucial, neutral document for senior executive decision makers at ports** who are responsible for safeguarding against **cybersecurity** risks as well as **ensuring** the continued business **resilience** of their organization.

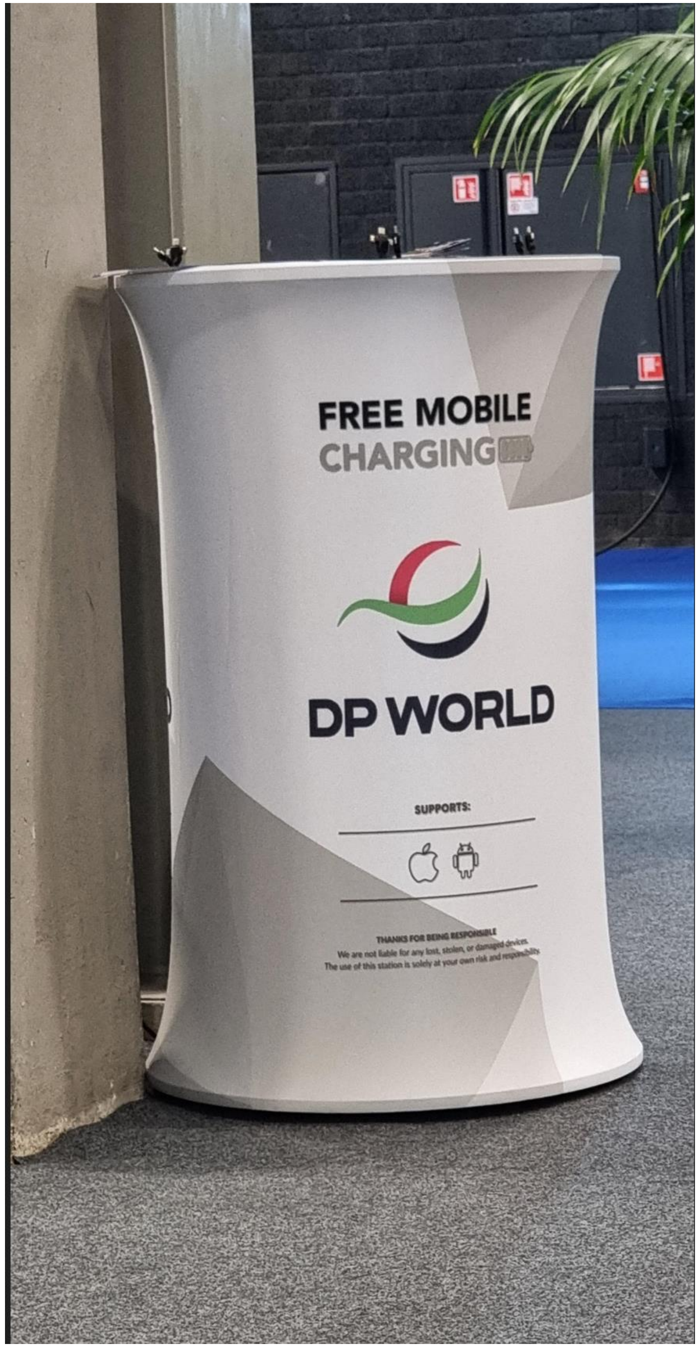


IAPH submissions endorsed at IMO FAL 46

May 30, 2022

The 46th meeting of the IMO Facilitation Committee (FAL 46) took place from 9 to 13 May. It was a successful meeting for IAPH with two submissions noted and approved by the Committee. Firstly, there was the paper by IAPH and co-sponsors BIMCO and IHMA proposing amendments to the Maritime Single Window Guidelines to include guidance on the port call process and the operational and nautical data that may be exchanged through a maritime single window. Secondly, IAPH had submitted a proposal inviting the Committee to note the first edition of the IAPH Cybersecurity Guidelines for Ports and Port Facilities and to consider promoting them as appropriate and referencing them in the next version of IMO's Guidelines on Maritime Cyber Risk Management. Both documents were met with appreciation from Member States and were approved accordingly. The FAL Committee also adopted amendments to the Facilitation Convention, which will make the Maritime Single




FREE MOBILE
CHARGING
DP WORLD
SUPPORTS:
THANKS FOR BEING RESPONSIBLE
We are not liable for any lost, stolen, or damaged devices.
The use of this station is solely at your own risk and responsibility.

The five essential steps towards cyber resilience

1

Port leaders should acknowledge cyber risk management as a top-level responsibility recognizing it as a competitive and operational imperative

2

Successful cyber risk management **begins with and depends on a common understanding of terms**, financial grounding, and recognition of shared responsibility

3

You cannot minimize the threat until you **understand the risk**

4

Protect, detect and mitigate

5

Work towards effective organizational **cyber awareness**

Step three

1

Port leaders should acknowledge cyber risk management as a top-level responsibility recognizing it as a competitive and operational imperative

2

Successful cyber risk management begins with and depends on a common understanding of terms, financial grounding, and recognition of shared responsibility

3

You cannot minimize the threat until you understand the risk

4

Protect, detect and mitigate

5

Work towards effective organizational cyber awareness

Assessing for Risk

Assess for vulnerabilities

To identify and evaluate the cybersecurity vulnerabilities within the complex operating environment of a port or port facility.

Assess for impact

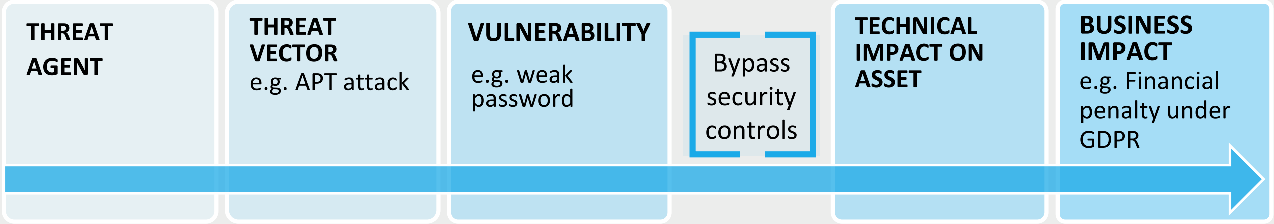
Impact refers to the potential harm that a cyber threat might cause to a port or port facility.

Assess for risk

To gain insights into the cyber risks to port and port facilities operations.

Risk identification

- Asset identification
- Understanding data as an asset
- Assess for threats
- Create risk scenarios



THREAT AGENT

THREAT VECTOR
e.g. APT attack

VULNERABILITY
e.g. weak password

Bypass security controls

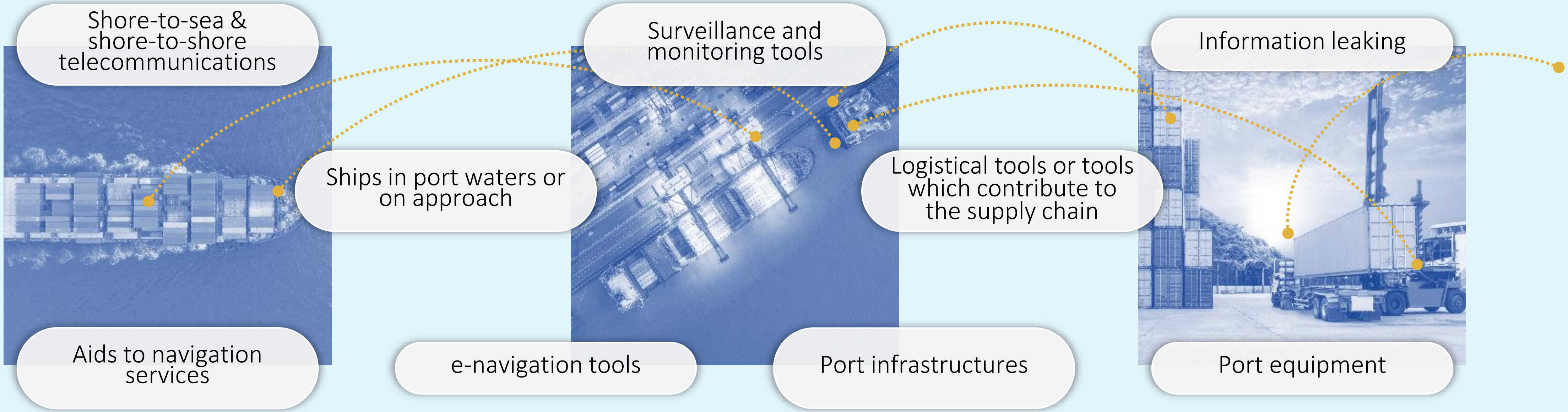
TECHNICAL IMPACT ON ASSET

BUSINESS IMPACT
e.g. Financial penalty under GDPR

- Risk analysis

Ports context : cyber vulnerabilities amplification

- Operational aspect:
  - Increased sharing of real-time data,
  - Interconnections with multiple stakeholders,
  - Complexity of business and OT systems
- Technical aspect: Difficulty in applying security updates / Continuous operation
- Smart Port trends : Increased exposure to cyberthreats



Shore-to-sea & shore-to-shore telecommunications

Surveillance and monitoring tools

Information leaking

Ships in port waters or on approach

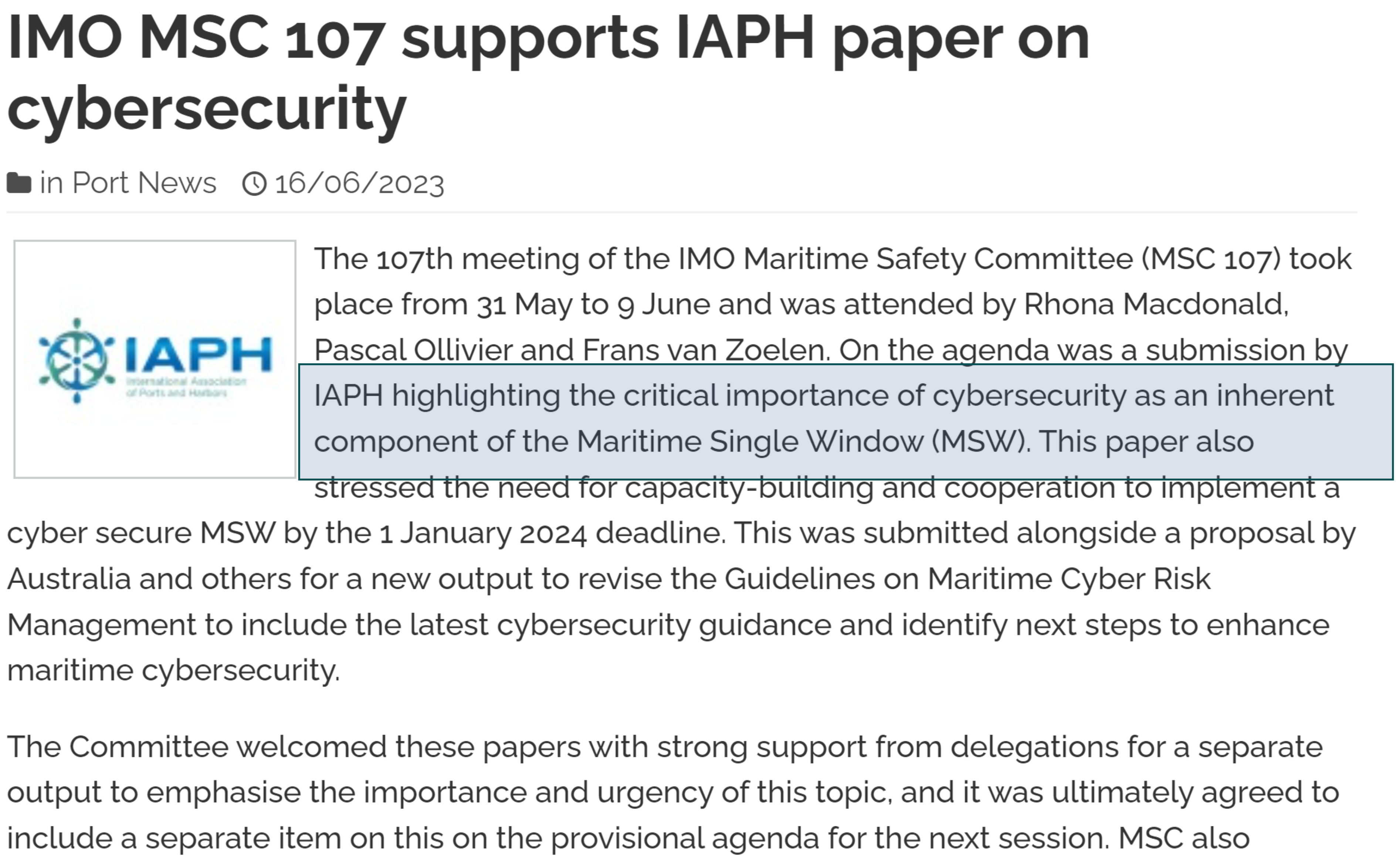
Logistical tools or tools which contribute to the supply chain

Aids to navigation services

e-navigation tools

Port infrastructures

Port equipment



IMO MSC 107 supports IAPH paper on cybersecurity

in Port News 16/06/2023

The 107th meeting of the IMO Maritime Safety Committee (MSC 107) took place from 31 May to 9 June and was attended by Rhona Macdonald, Pascal Ollivier and Frans van Zoelen. On the agenda was a submission by IAPH highlighting the critical importance of cybersecurity as an inherent component of the Maritime Single Window (MSW). This paper also stressed the need for capacity-building and cooperation to implement a cyber secure MSW by the 1 January 2024 deadline. This was submitted alongside a proposal by Australia and others for a new output to revise the Guidelines on Maritime Cyber Risk Management to include the latest cybersecurity guidance and identify next steps to enhance maritime cybersecurity.

The Committee welcomed these papers with strong support from delegations for a separate output to emphasise the importance and urgency of this topic, and it was ultimately agreed to include a separate item on this on the provisional agenda for the next session. MSC also

Smart Port trends – Supporting Cybersecurity Resilience

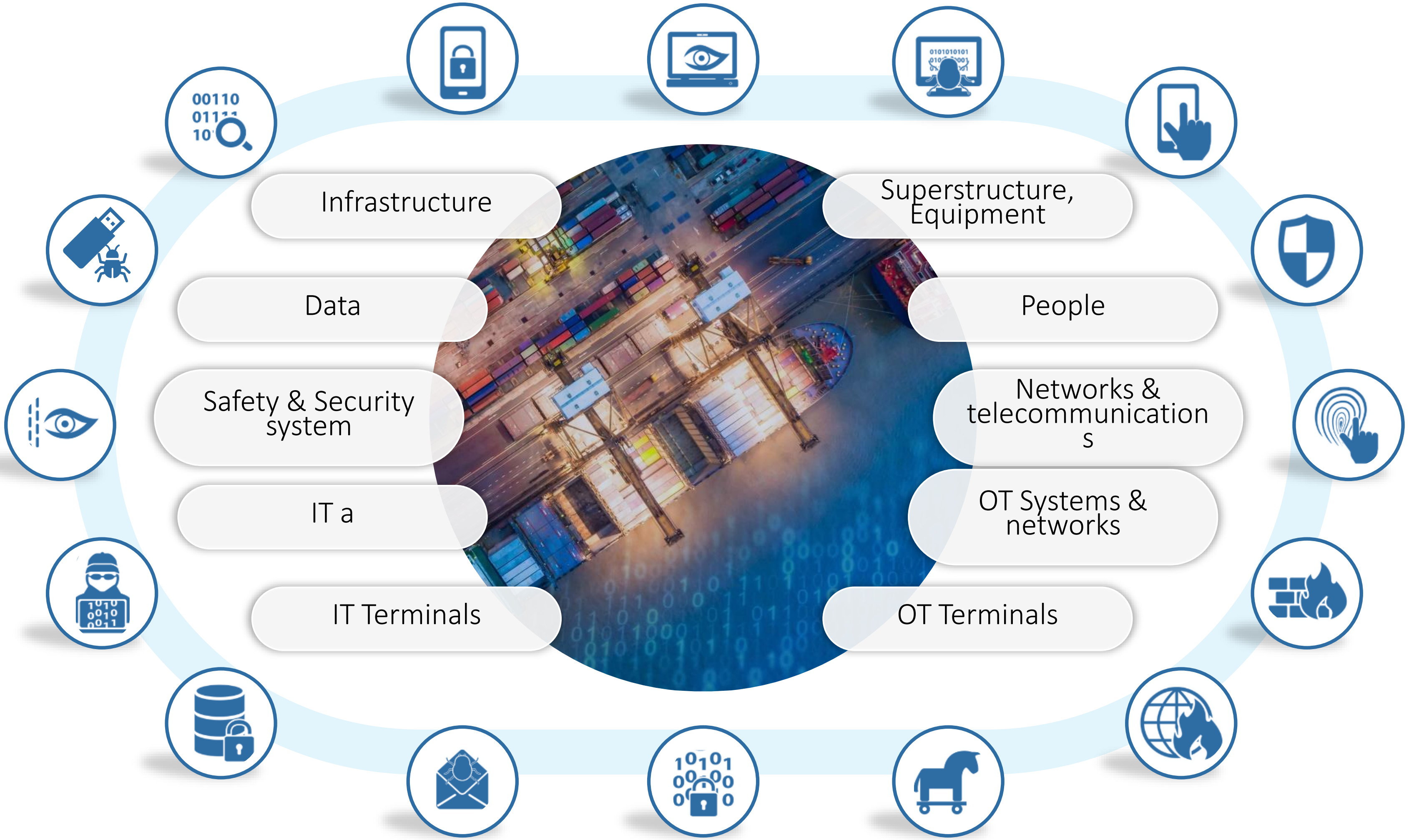
Smart Container use case:
Yard inventory count and registration

- Suppose that because of a cyber-attack the TOS database can’t be restored and, as a result, there is a need to manually count and register the inventory of thousands of containers in the port yard.
- However, if the yard is filled with Smart Containers that can instantly transmit their identification numbers and locations, the TOS database can be immediately updated.
- This can save many hours of manual work and enable a quick recovery from the cyber-attack.

Difficulty in mobilizing a port stakeholders community on cyber issues

- Many stakeholders to coordinate,
  often interdependent
- Business ecosystem relying on
  multinational companies & very small enterprises
- Professionals under pressure,
  often behind their schedule
- Narrow Vision, silo working
- Low interest in cybersecurity topics

Physical & non-physicals impacts



iaph

Shipping industry expects cyber-attack deaths, collisions, and groundings

DNV

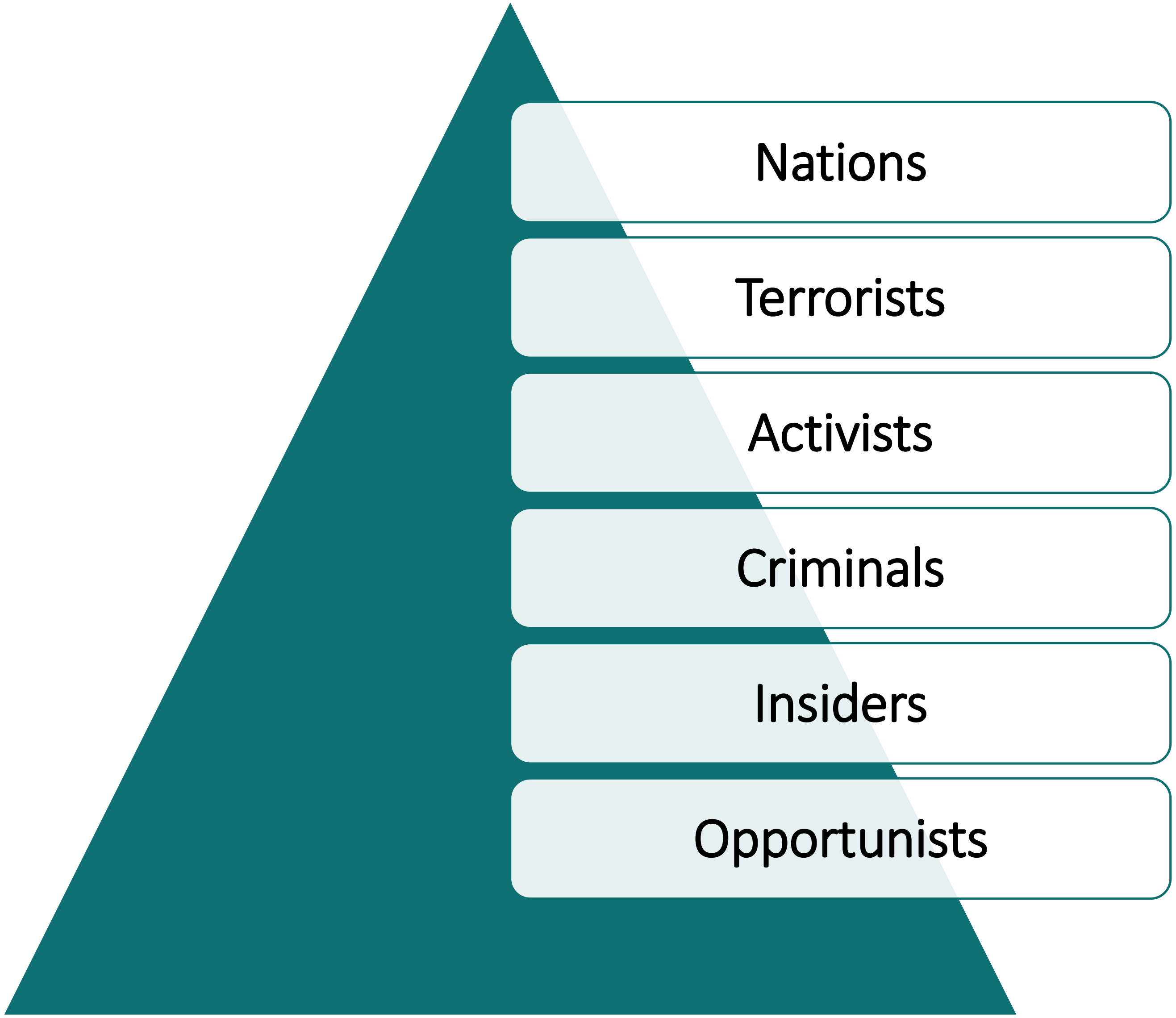
Maritime cyber security needs more investment, better regulation, and sharing of incident experiences, according to a DNV report.

Gary Howard | Jun 06, 2023

As well as enabling threat actors to demand ransom, steal intelligence and cause widespread disruption – which hackers can also achieve by breaching IT networks – attacks on OT systems can disable assets or safety controls. Indeed, 56% of maritime professionals expect cyber-attacks to cause physical injury or death in the industry within the next few years.

https://www.seatrade-maritime.com/technology/shipping-industry-expects-cyber-attack-deaths-collisions-and-groundings?trk=feed_main-feed-card_feed-article-content

Cyber pirates



Nations

Terrorists

Activists

Criminals

Insiders

Opportunists

Defining the Organization’s Cyber Ecosystem: Activities & Stakeholders

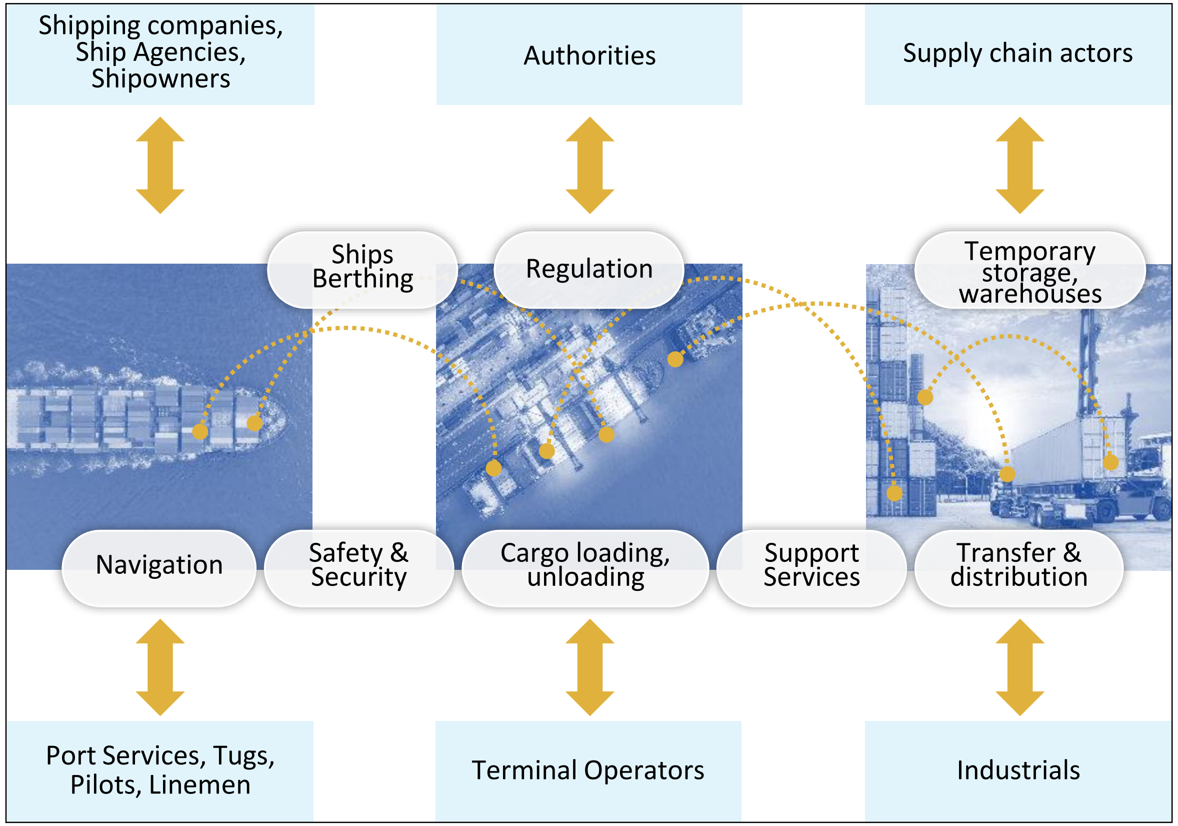
In order to manage their cyber risk port and port facility leaders must first understand what are the most critical operational activities, and who are the individual stakeholders supporting them.

Critical Activities:

- Activities linked to sea freight and hinterland transport (e.g. unloading and loading, etc.)
- Activities related to the transport of passengers and vehicles (e.g. border control, etc.)
- Activities related to traffic coordination (e.g. AIS, etc.)
- Industrial activities (e.g. petrochemicals, etc.)
- Fishing related activities (e.g. inspection of fish, etc.)

Critical Stakeholders

- Ocean transportation (e.g. shipping companies, etc.)
- Authorities (e.g. port authority, customs,, etc.)
- Supply chain (e.g. freight forwarders, etc.)
- Terminal operators
- Port service providers (e.g. tug operators, etc.)
- PCS operators
- Industrial (e.g. petrochemicals, etc.)



Defining the Organization’s Cyber Ecosystem: Assets

Critical Assets – Data exchange/Systems and tools

- Mandatory declarations (e.g. FAL forms, etc.)/ (e.g. MSW, etc.)
- Control and authorization (e.g. custom clearance, etc.)/ (e.g. PCS, etc.)
- Operational data related (e.g. freight scheduling, etc.)/ (e.g. TOS, etc.)
- Financial and business data (e.g. invoicing,, etc.)/ (e.g. Billing, etc.)
- Navigation and traffic management data (e.g. AIS, VTS, etc.)

Port and port facility cyber ecosystems are **dynamic** and its stakeholders are highly interdependent. Therefore, **periodic review** of the ecosystem critical **activities/stakeholders/assets** and making appropriate adjustments, are recommended

iaph

Cybersecurity is not just for the IT department

1 Cyber risk is an enterprise-wide risk

Cyber risk is pervasive. Cyber risk factors **touch every aspect of the organization** including administration and operations. Cyber risk management only succeeds with the active executive engagement and oversight.

2 People are the weakest link in cyber risk management

Managing cyber risk encompasses people, technologies, processes. Cyber threat actors commonly target **non-IT staff, which represents the majority** of an organization's personnel.

3 **The impact of cyber breaches can be disastrous**

The consequences of compromised port and/or port facilities' digital processes could result in operational disruption, affecting customers, port authorities, port community systems, and related port services.

Cyber resilience requires pre-defined decisions and pre-defined cooperation

coordinated with all the stakeholders,

inside and outside the port

iaph

Israeli Maritime-Tech Startups*

Logistics & Supply Chain

WAVE BL

AiDock From Docs to Docks

FREIGHTOOLS POWERED BY FAST

wisor

LADINGO

CartaSense

CENTGUARD SHIPPING WITH INTELLIGENCE

FREIGHTOS Smooth shipping

Guarda

NEO COMPOSITE

SAMSON LOGIC Smart solutions for construction logistics

GO TRACK

TRUCKNET

GearEye

SHIPPI

shipit.to

BRINGG

STARGO

ALLFORWARD

FOXinGREEN just for it

YASHAR

LOGINNO

CARGOSYS SIMPLIFY YOUR SHIPPING

SODYO The O2O Infrastructure Solution

CARGOZONE

NEMODATA

hoopo

Tomindu

bizWatch

Convaze last mile solutions

Sealogic bv Global Freight Forwarding

Bringoz Right here Right now

Leisure (Cruise, Marinas)

Pick a Pier

seazone

ZCT

SIGHTBIT

BoatClick

LYNXIGHT DEEP VISION

SEA ANALYTICS

ROUTIER COMMUNICATION DONE RIGHT

hopa

ManageYourTrip

RightHear

AHOY! INSURANCE Insurance by sailors for sailors

LEVEL

econet

Cyber & HLS

ArcusTeam

NavalDome maritime cyber defense solutions

MAGOS

SCADAfence

TRACETECH SECURITY LTD

MAGAL SECURITY SYSTEMS

cervello

InfiniDome THE GPS CYBER COMPANY

ARGUS CYBER SECURITY

Cyberstar

WATERFALL Stronger Than Firewalls

REGULUS

AIROBOTICS

OTORIO

APOLLOSHIELD

skysapience

CYDOME

PRISMA PHOTONICS

PERCEPTO

COPTER PIX PRO AUTONOMOUS DRONES ADVANCED SOLUTIONS

Operational Optimization & InsurTech

DOCK TECH THE FUTURE OF DEPTH

CAPTAIN'S EYE

MASSIVit 3D

OFIL

3DIN Simply Expand

tomorrow.io

AQUANT

WINDWARD

3dSignals

Spectralics

IntellAct

CIPHERSIP

Mobi Mobility Insight

KARDOME

SuperiorFINS

STARCOM Systems

AERO DRIVETRAIN FLUID IN MOTION

viisights Intelligence by vision

connecteam

FIELDBIT

FIRST AIRBORNE

AUGURY

PLATAINE people-smart automation

thermoSiv Heat makes sense

GOARC

Autonomous Vessel & Smart Port

ORCA AI

ASIO

ottopia

TotemPlus Where Shipping Meets High-Tech

UltraWis

AutonomEES Energy Exchange Systems

SEALARTEC

BG ROBOTICS

DEEYOOK

SeaErra

INTSITE

Environment & Safety

ECOncrete Concrete Ecological Solutions

GiliOcean Technology

Eco Wave Power

NAYAM WINGS MARITIME WIND PROPULSION

kando

Electriq Global

APOLLO POWER

OBS Ocean Bricks Marine Structures

MARINE EDGE

Balast Marine LTD

plasticback

* The chart comprises of "pure-play" maritime startups, as well as startups attending different industry but have a strong maritime use case.

THE DOCK THE MARITIME INNOVATION PORT OF CALL

January 2022

Marinnovators Consulting Services: Digital Transformation, Innovation, Cybersecurity

Cyber Solutions

- Cydome
  Cyber Security Coverage for Protecting IT & Operational Assets in Ships and Ports while assuring their readiness for regulatory inspections.

- Salvador:
  Solutions for operational continuity and cyber-attack recovery in SCADA and HMI systems

- Cyberstar:
  A cybersecurity company, subsidiary of ZIM, the Israeli shipping line, offering Cybersecurity services such as cyber-attack simulation, cybersecurity gap analysis, etc.

- EasySec
  Endpoint Protection for Industrial IoT and Control Systems

Thank you for your attention!

For your copy of the guidelines:

https://bit.ly/IAPHCyberGuide1

For more information, contact:

gadib@marinnovators.com

To join IAPH and its Data Collaboration Technical Committee, contact:

antonis.michail@iaphworldports.org

The biggest room in the world, is the room for CYBER improvement

Gadi Benmoshe

Vice-Chair IAPH DCC, Managing Director, Marinnovators

gadib@marinnovators.com
+972-506460980