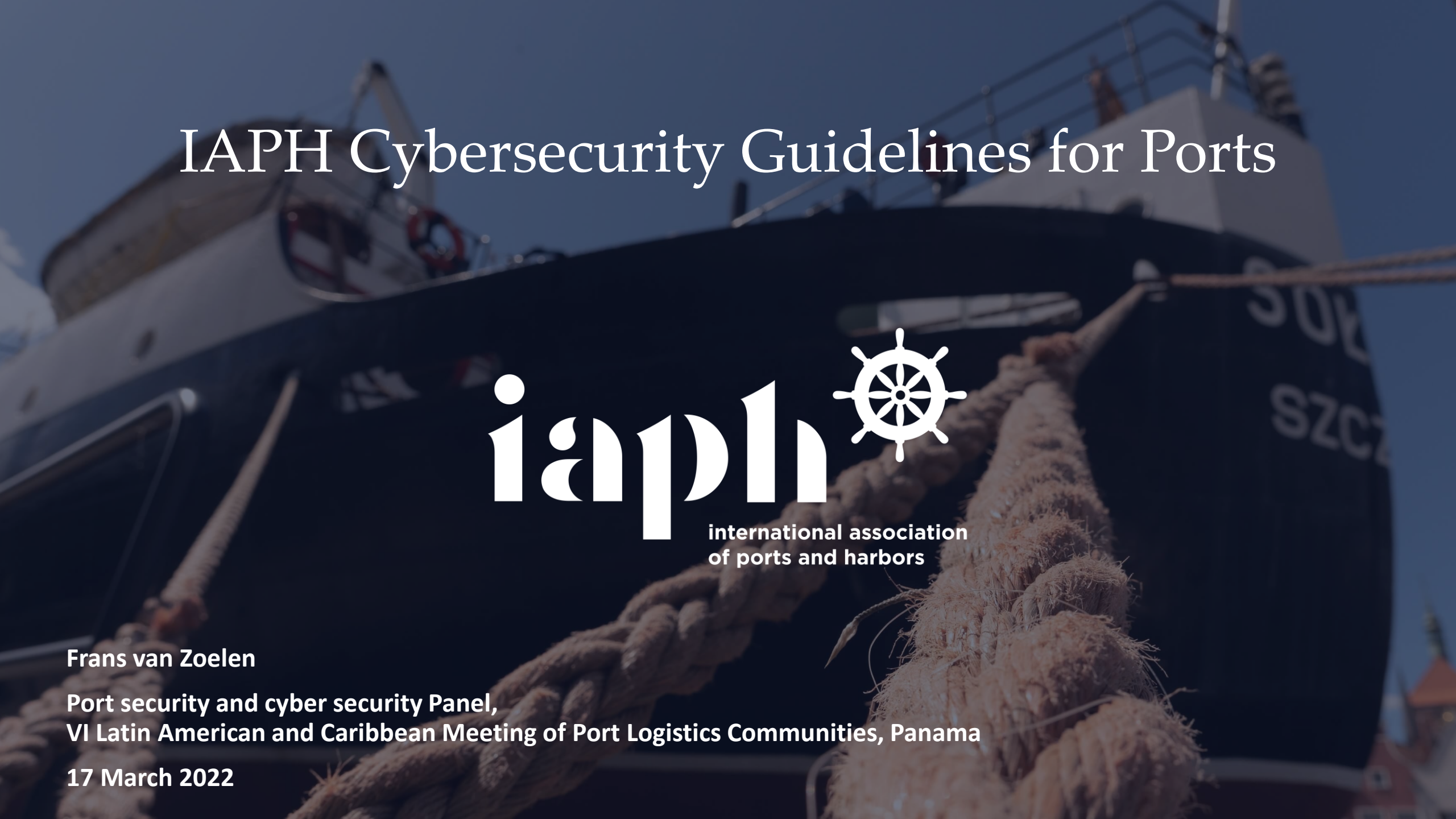
IAPH Cybersecurity Guidelines for Ports



international association
of ports and harbors

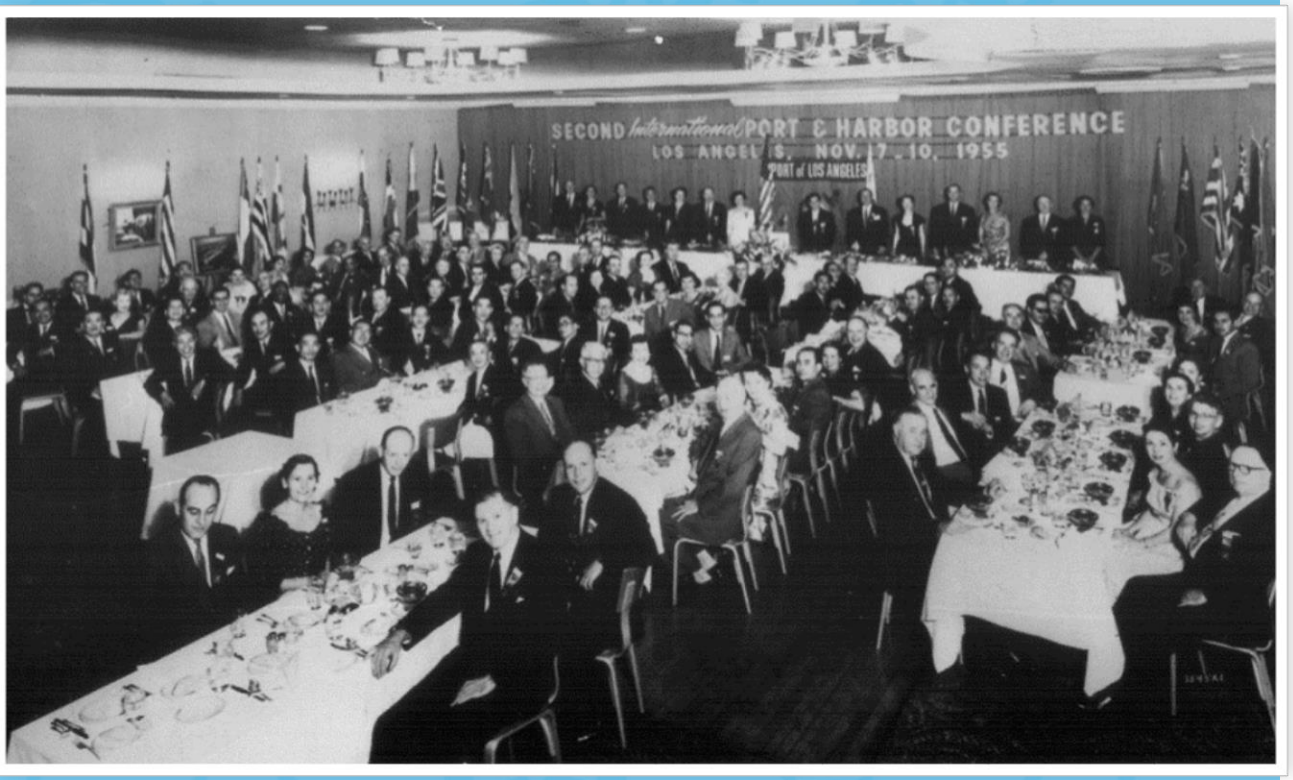
Frans van Zoelen

Port security and cyber security Panel,
VI Latin American and Caribbean Meeting of Port Logistics Communities, Panama

17 March 2022

Introduction to IAPH

Q1 2022



Founded in 1955, IAPH represents global port authority and port operator interests on a regulatory level at the International Maritime Organization (IMO), presenting submissions and commenting papers to its main Technical Committees and participating in it's principal working groups

IAPH has consultative status and works on behalf of ports with additional United Nations bodies such as the ILO, UNCITRAL, UNCTAD (UN Conference on Trade and Development), UNEP (UN Environment Program) and the UN Global Compact.

IAPH collaborates with other NGOs and Associations such as the World Customs Organization, the Global Maritime Forum and the World Economic Forum. It also closely collaborates with the World Bank.

Over the past six decades, IAPH has developed into a global alliance of ports, representing today some 162 regular port members and 126 port-related associate members in 87 countries.

Member ports together handle well over one third of the world's sea-borne trade and over 60% of the world container traffic.

Further to a change of constitution in 2016, IAPH has strategically reoriented its focus outwards from its port base, engaging with port community stakeholders running throughout the maritime transport chain. With the outbreak of the global pandemic, IAPH's COVID19 Taskforce tracked developments across the world's ports, with member experts in all functions sharing best practices and experiences in keeping ports operational.

iaph

THEMES

Climate & Energy

IAPH occupies an influential seat at the table of the International Maritime Organization, with both shipping and ports now beginning to open meaningful dialogues together on climate action, digitalization, trade facilitation and environmental performance.

Data Collaboration

IAPH has taken a front-running role in a joint industry call to accelerate digitalization. This policy document was issued in June 2020, co-signed by leading maritime industry associations and endorsed by the IMO Secretary General.

Risk & Resilience

Following the outbreak of the COVID-19 pandemic, IAPH set up a COVID-19 Taskforce composed of some of the world's leading port experts in operations and crisis management, combined with specialists called upon to make contributions

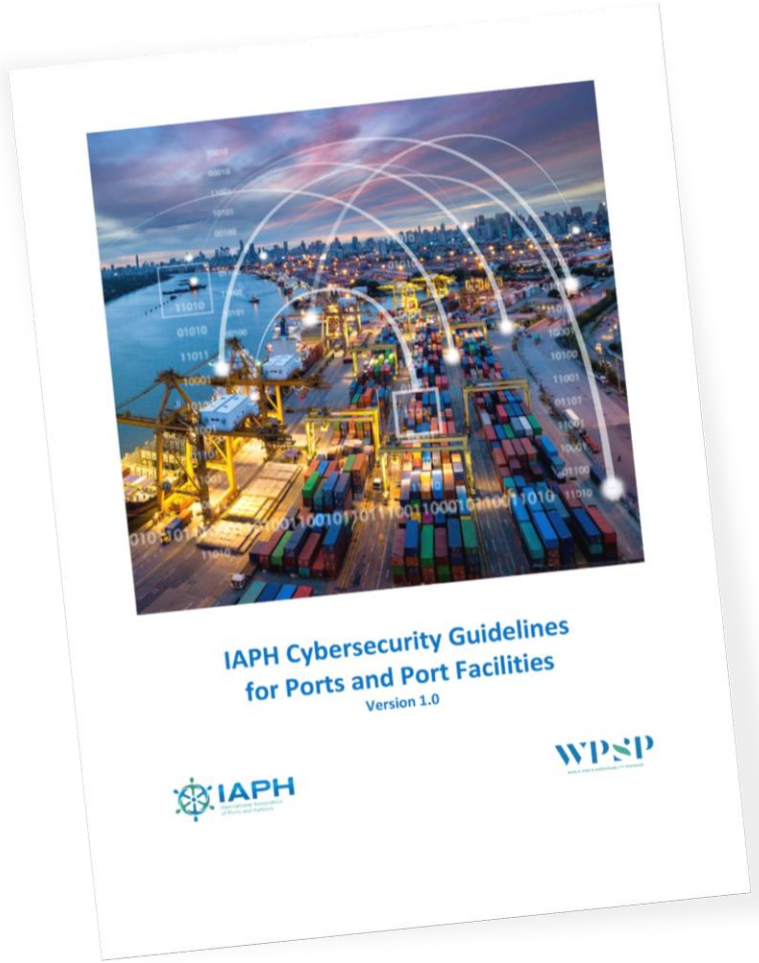
The IAPH Data Collaboration Committee

	TOPIC	FOCUS/PURPOSE	DELIVERABLES
1	Acceleration of digitalisation (priority actions joint industry statement June 2020)	Work with World Bank, IMO and others in setting up a capacity-building project for ports in emerging and developing countries	Project plan
		Status of implementation in ports	Dashboard
		Sharing best practices in a structured way	Database
		Facilitate dialogue with ports, shipping and standardisation bodies on common data sets	Roadmap
2	IMO Facilitation Convention (FAL)	Support implementation FAL requirements	Submissions and interventions
		Support adoption of common administrative and operational data standards (port call optimisation)	
3	**Cybersecurity**	**Publication and submission to IMO of Port and Port Facility Cybersecurity Guidelines**	**Submissions and interventions**
4	Automation	IAPH positioning in Maritime Safety Committee (MSC)	Submissions and interventions
5	Innovation	Facilitate the emergence of startups on a global scale to facilitate data collaboration and smart ports	Platform

iaph

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. It will 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.



What is the aim of the document ?

- The document aims to assist ports and port facilities to establish the true financial, commercial & operational impact of a cyber-attack.
- It also is intended to help ports and port facilities make an objective assessment on their readiness to prevent, stop and recover from a cyber-attack.
- The Guidelines also address the very difficult question of what port organizations need in terms of resources to effectively manage cybersecurity risks.

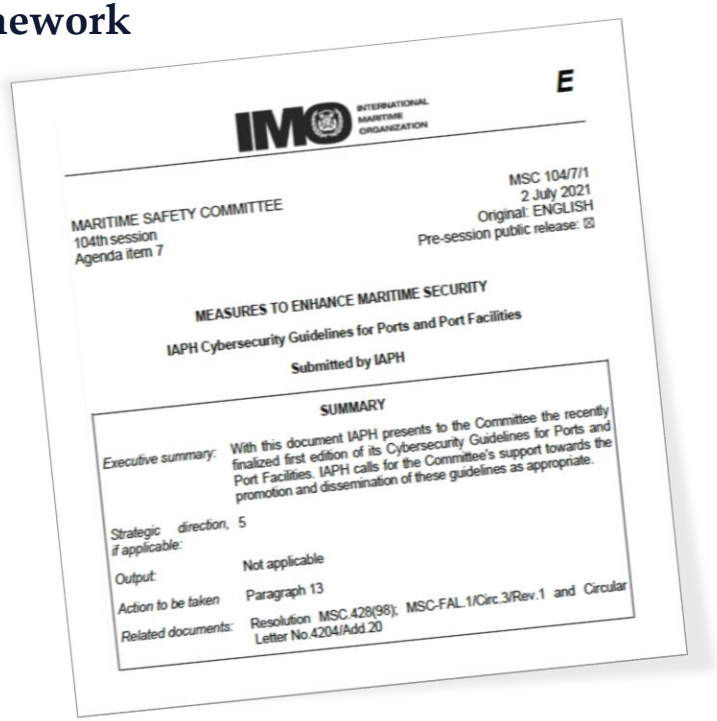
Regulatory Status of IAPH Cybersecurity Guidelines for Ports and Port Facilities

- Industry guidelines
- MSC-FAL.1/Circ.3 5 July 2017 Guidelines on Maritime Cyber Risk Management

  Section 4: Paragraph 4.2. Best Practices for Implementation of Cyber Management

  BIMCO Guidelines, ISO/IE 27001, NIST Framework

  Plus: **IAPH Cybersecurity Guidelines**



E

IMO INTERNATIONAL MARITIME ORGANIZATION

MARITIME SAFETY COMMITTEE
104th session
Agenda item 7

MSC 104/7/1
2 July 2021
Original: ENGLISH
Pre-session public release: ☒

MEASURES TO ENHANCE MARITIME SECURITY

IAPH Cybersecurity Guidelines for Ports and Port Facilities

Submitted by IAPH

SUMMARY

Executive summary: With this document IAPH presents to the Committee the recently finalized first edition of its Cybersecurity Guidelines for Ports and Port Facilities. IAPH calls for the Committee's support towards the promotion and dissemination of these guidelines as appropriate.

Strategic direction, if applicable: 5

Output: Not applicable

Action to be taken: Paragraph 13

Related documents: Resolution MSC.428(98); MSC-FAL.1/Circ.3/Rev.1 and Circular Letter No.4204/Add.20

- Non-mandatory, but
  - Endorsed by IMO in 2021/2022 via MSC-104 and FAL-76 and to be mentioned in MSC-FAL.1/Circ.3
  - Objectivized method of working
  - Objectivized referential character in context of i) insurance and ii) aftermath of an incident
- Significant from a regulatory perspective:

  - offers a way for inclusion cybersecurity assessment into the Port Facility Security Plan

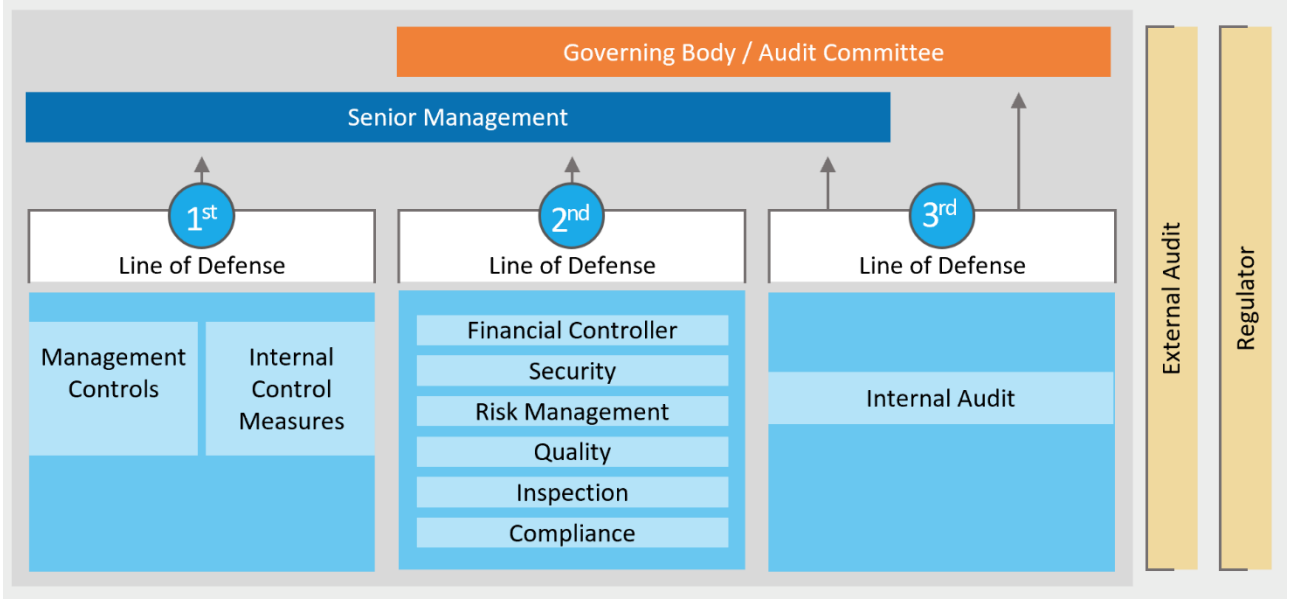
  - stepping stone to come to external info sharing on cybersecurity threads

iaph

Cybersecurity and risk management – setting up the internal governance (1)

Three Lines of Defense model helps in creating the right responsibility within the organization:

- 1st Line implementing controls, adhering to policies and risk owner
- 2nd Line developing, facilitating and monitoring the 1st Line
- 3rd line involves auditing the 2nd Line



Cybersecurity and risk management – setting up the internal governance (2)

Legal Audit on cybersecurity issues:

1. Is a cyber attack still considered as force majeure in your circumstances?

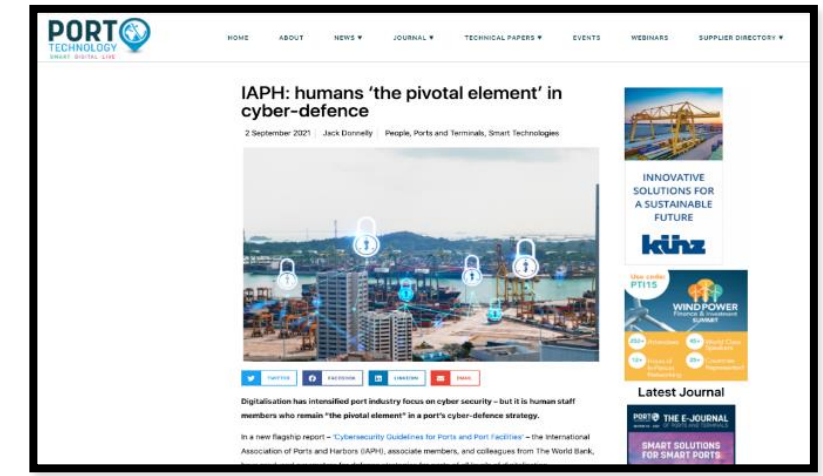
2. Check:
   - General Conditions for using your port
   - Lease contracts with stevedoring companies

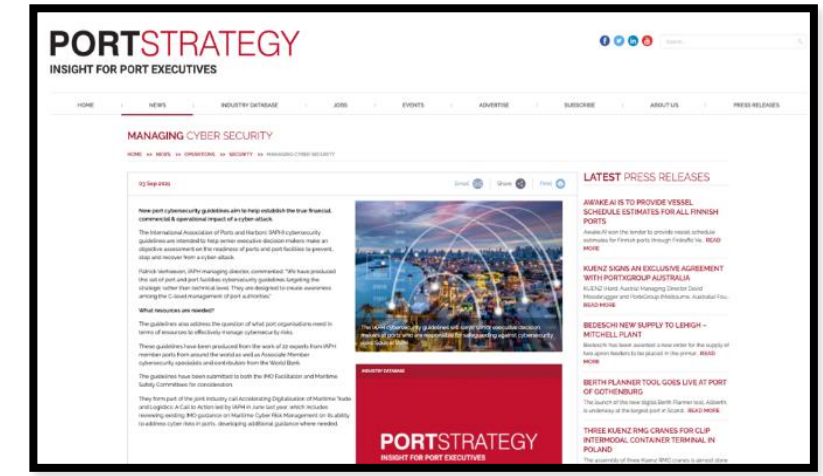
3. Check insurance policies:
   - liability and business interruption insurances

4. Cyber attack exercises with all disciplines involved

IAPH Cybersecurity Guidelines have received a lot of attention

- Over 1,300 downloads since launch from the World Ports Sustainability Program website
- Extensive sector coverage, also in the mainstream cybersecurity community





Thank you for your attention!

For your copy of the guidelines:

https://bit.ly/IAPHCyberGuide1

For more information, contact:

FJW.Zoelen@portofrotterdam.com

As of May 2022, Mintco Legal Consultancy:

fransvanzoelen@chello.nl

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

antonis.michail@iaphworldports.org

iaph