Cybersecurity and the Maritime Single Window (MSW, mandatory from 2024)

iaph

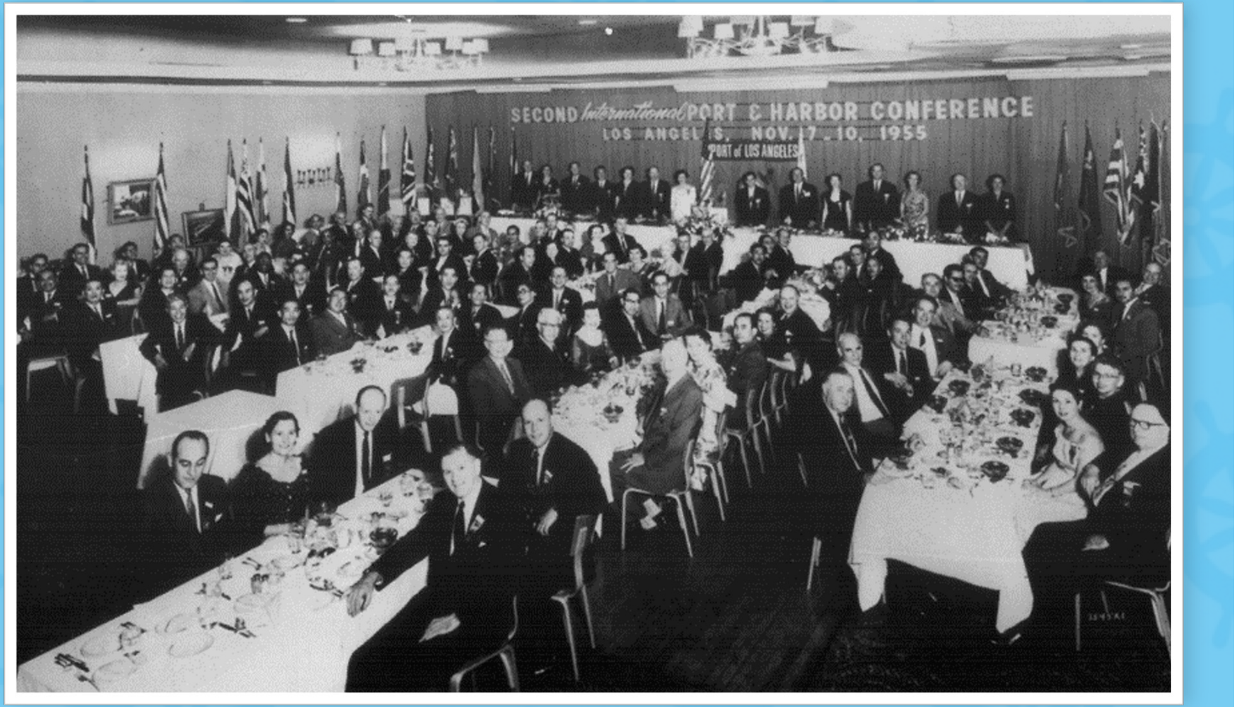
international association of ports and harbors

IMO/UNIVERSITY OF PLYMOUTH (Cyber-SHIP Lab) SYMPOSIUM
"MARITIME CYBER SECURITY AND RESILIENCE"
1 and 2 November 2023 at IMO

Frans van Zoelen

Content of Presentation:

1. International Association of Ports and Harbors (IAPH)
2. How do cybersecurity resilience improving instruments (mandatory/non-mandatory) reach the maritime and port domain?
3. IAPH Cybersecurity Guidelines for Ports and Port Facilities
4. Roadmap to cybersecurity legislation at national levels
5. Accelerating cybersecurity resilience in context MSW
6. Concluding remarks


SECOND International PORT & HARBOR CONFERENCE
LOS ANGELES, NOV. 7-10, 1955
PORT of LOS ANGELES

1 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.

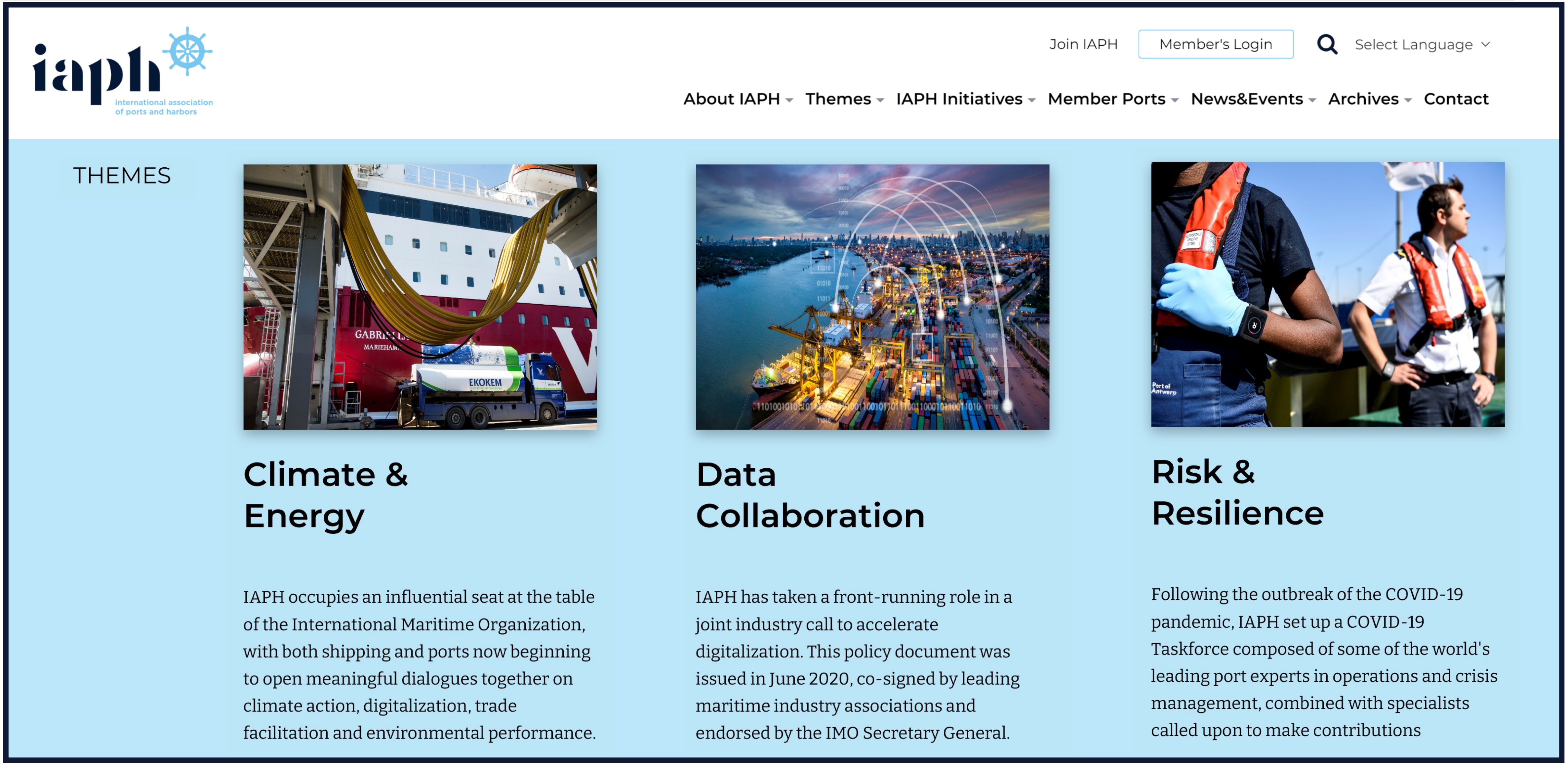
2 IAPH has consultative status and works on behalf of ports with additional United Nations bodies such as the ILO, UNCITRAL, UNCTAD (UN Conference on Trade and Development), UNEP (UN Environment Program) and the UN Global Compact.

3 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.

1 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.

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

3 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.



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

How do Cybersecurity Instruments (mandatory/non-mandatory) reach the maritime and port environment? (1)

1 Via non-mandatory (industry) guidelines:

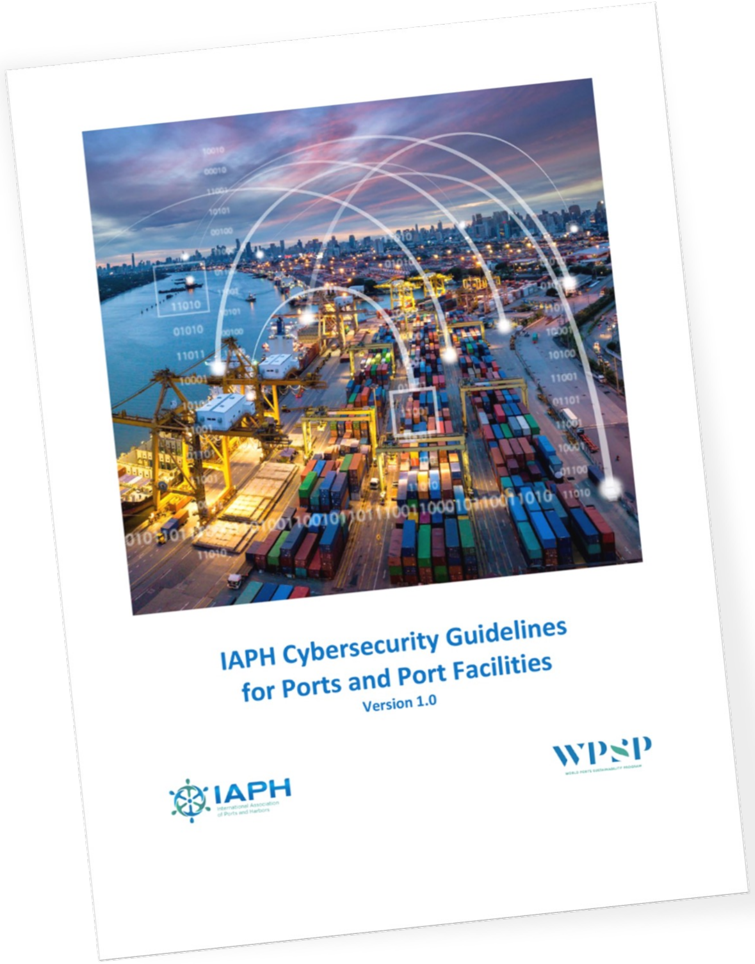
- IAPH Cybersecurity Guidelines for Ports and Port Facilities
- Guidelines on Cyber Security Onboard Ships, by ICS, IUMI, BIMCO et cetera

2 IMO Guidelines on Maritime Cyber Risk Management (MSC FAL.1/Circ.3/Rev.2)

> "For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices." (Section 1.3)
>
> "These Guidelines are primarily intended for all organizations in the shipping industry, and are designed to encourage safety and security management practices in the cyberdomain." (Section 2.2.1)

What are the IAPH Cybersecurity 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.



IAPH Cybersecurity Guidelines for Ports and Port Facilities

Version 1.0

IAPH

WPSP

What is the aim of the document ?

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

Content of IAPH Cybersecurity Guidelines for Ports and Port Facilities more specific

1. Reason why cybersecurity is a serious and a very relevant topic
2. Risk management related to cybersecurity
3. Overview of possible cyber threats for ports and port facilities
4. Preventive measures and possibilities to recognize potential attacks
5. Information sharing and information sharing basics
6. Training schemes
7. Incident management and recovery after a cyber incident
8. Template for a Port Facility Cybersecurity Assessment (via PFSA/PFSP of ISPS)

How do Cybersecurity Instruments (mandatory/non-mandatory) reach the maritime and port environment? (1)

1 Via non-mandatory (industry) guidelines:

- IAPH Cybersecurity Guidelines for Ports and Port Facilities
- Guidelines on Cyber Security Onboard Ships, by ICS, IUMI, BIMCO et cetera

2 IMO Guidelines on Maritime Cyber Risk Management (MSC FAL.1/Circ.3/Rev.2)

> “For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments’ and Flag Administrations’ requirements, as well as relevant international and industry standards and best practices.” (Section 1.3)

> “These Guidelines are primarily intended for all organizations in the shipping industry, and are designed to encourage safety and security management practices in the cyberdomain.” (Section 2.2.1)

How do Cybersecurity Instruments (mandatory/non-mandatory) reach the maritime and port environment? (2)

3 ENISA – Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector (2019)
ENISA – Cyber Risk Management for Ports (2020)

4 Via non-mandatory Standardization, Recommendation and Certification Systems:

- ISO/IEC 27001
- Consolidated IACS Recommendation on cyber resilience (Rec 166)
- NIST Cybersecurity Framework (2.0 in draft)
- CISA Cross-Sector Cybersecurity Performance Goals for Critical Infrastructure Entities (applying NIST CF)
- US DoD's Cybersecurity Maturity Model Certification (CMMC) for Defense Industrial Base Sector

5 Via *mandatory* ISPS:

- concerns only port facilities
- if assumed cybersecurity is a relevant formal element in ISPS and should be addressed in the PFSA/PFSP

How do Cybersecurity Instruments (mandatory/non-mandatory) reach the maritime and port environment? (3)

6 Via ***mandatory*** cybersecurity legislation in various jurisdictions which protect:

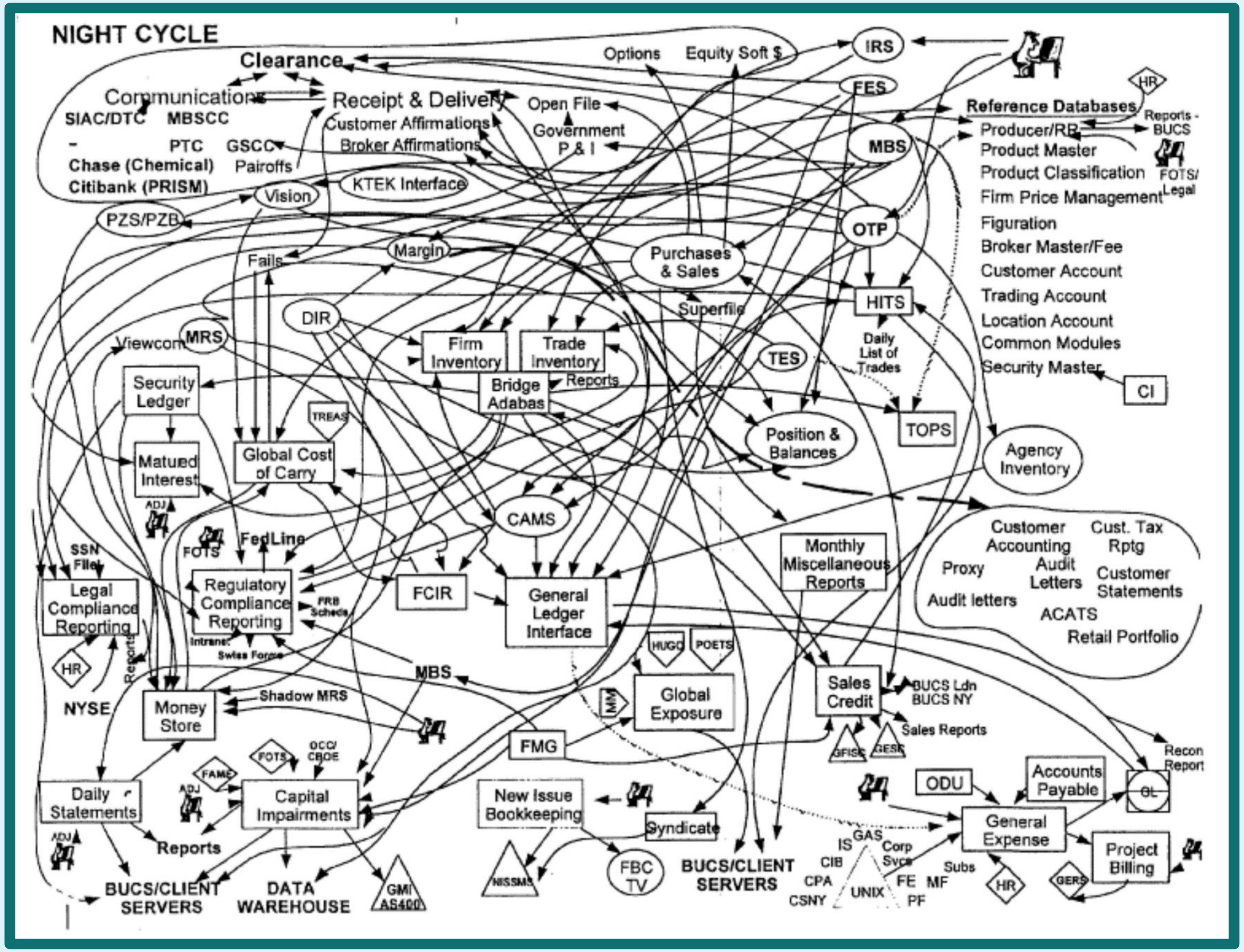
- Network and Information Systems Security Frameworks
- Critical Entities or Critical Infrastructures Protection Frameworks

Relevant if port and maritime entities are under the scope of these mandatory systems.

Overview (although often scattered over different parts and areas of law)

- India (The Information Technology Act 2000), Brasil (Cybersecurity Regulation), Ghana (Cyber Security Act 2020), US (USCG MTSA requirements, some State requirements, + CBP, MARAD, TSA, and more), Singapore (Cybersecurity Act), UK (NIS1), China (Cybersecurity Law)
- EU Network and Information Security Directive (NIS1 and NIS2) – so far as maritime and port entities are defined under the scope of these directives
- EU Critical Entities Resilience Directive – so far as a maritime or port entity is defined as a critical entity under the scope of this directive

Roadmap to cybersecurity legislation at national level



Roadmap to cybersecurity legislation at national level (2)

1. Process
2. Scope of legislation
3. Definition of legal obligations
4. Notification, supervision and reporting requirements incidents
5. Information sharing

Roadmap to cybersecurity legislation at national level (3)

Process

Establish a lead agency:

- Which is strong, resourceful and empowered to guide this specific legislation project through the different phases in an integrated way.
- Which understands the value proposition of cybersecurity and is able to liaise with key organizations.
- Normally: Ministry of Justice. But this does not imply the executing government agency is also the MoJ; could be Ministry of Trade, or Economic Affairs, or (a) special agenc(y)(ies), or a combination, depending on national situation.
- Which understands the culture of legislation in the specific jurisdiction on this specific point.

Keep in mind structure and flexibility of legislation:

- Because of volatile nature of cybersecurity: sufficiently adaptive and future-proof.
- Implementing the specific operational measures into lower hierarchy of law.

- Aim at clear and transparent allocation of competences between government agencies:
  - Regulatory
  - Guidance
  - incident response and auditing
  - enforcement

Roadmap to cybersecurity legislation at national level (4)

Scope of legislation (1)

- Horizontal or vertical approach: General or Sector Specific Legislation
- Combination: Sector Specific Legislation and General Legislation (excluding entities under SSL)

- Critical Infrastructure/Entities approach: specific legislation for “crown jewels” of a national economy. Demands an all-in approach with wider scope than only digital: digital, economic (merger and acquisition control), financial and physical threats protection.

Which entities to focus on when choosing General Legislation approach?

Not all, differentiate on basis of vital processes to define more specific the target audience:

Service provider driven approach:

Essential Service Providers
Digital Service Providers

Sector driven approach:

Essential sectors and important sectors
Or:
Very critical sectors and other critical sectors

Roadmap to cybersecurity legislation at national level (5)

Scope of legislation (2)

Size capping – no size capping in case of only one service provider

Within these groups applying different regimes:

- pro-active supervision or reactive monitoring
- intensity stretch by competent agency in case of incident response

Roadmap to cybersecurity legislation at national level (6)

Definition of legal obligations

Defining duty of care

Result should be: the target entities will take appropriate and proportionate technical, operational and organizational measures for addressing cybersecurity risks.

Spectrum for defining the duty of care:

1) Open approach: risk- and principal based, right-fitting to the organization
2) Closed approach: certification based approach

If (1) then guidance to safeguard minimum focus on cybersecurity measures:

- technical, operational, organizational level
- if compromised how to restrict, solve and report the incident

Roadmap to cybersecurity legislation at national level (7)

Definition of legal obligations (2)

In open (risk-based) system nevertheless addressing mandatory focus points:

a) Development and implementation of policies for risk analysis and information systems security

b) Incident response

c) Business continuity including disaster recovery and crisis management

d) Supply chain security (main vendors, how far back in the chain?)

e) Security re acquisition, development and maintenance network – and information systems – vulnerable strategic dependencies

f) Evaluation policies to assess effectiveness of cybersecurity risk-management

g) Human resources policies: basic training and incident response exercises

Roadmap to cybersecurity legislation at national level (8)

Definition of legal obligations (3)

In open (risk-based) system nevertheless addressing mandatory focus points:

h) Policies for cryptography including encryption

i) Security of hardware: screening, access control, asset management policies

j) Policies for multi-factor authentication (broad)

k) Internal governance structure of entities: CISA?

l) Defining scope of liability of Board of entities if infringements of cs-obligations of entity

m) Merger/Acquisition Control sensitive and critical entities

n) Information sharing structures on local and peer level (Port Community Systems)

Roadmap to cybersecurity legislation at national level (9)

Notification and reporting requirements of incidents

What is an incident?

- Event with *actual* adverse impact?
- Event which *could cause* adverse impact?
- Difference between incidents: *incidents* and *significant incidents*?
- Is *a cyberthreat as such* a relevant incident?

Notification models:

- Differentiation between an incident and a *significant* incident
- Significant incident: involvement *special response teams* for monitoring, analyzing, coordination and control
- Response teams: centralized and/or sectoral

Differentiation in timing regime of notification and reporting incidents:

- Immediately within q hours (after being aware) of an incident (early warning)
- Immediately within q hours reporting the initial assessment and possible impact
- Within q days the final report or progress report

Roadmap to cybersecurity legislation at national level (10)

Notification, supervision and reporting requirements of incidents (2)

Reporting to whom?

- Competent agency/agencies
- Response teams
- Relevant customers or relevant vendor
- Peer group – creating communities on local or functional level, or via Port Community Systems

Supervision and enforcement

- Audit rights
- Requests for information
- Binding instructions in case of negligence or infringement

Other considerations

- Contractual obligations, e.g. insurers
- Ethical obligation to inform the broader community (public/media)?

Roadmap to cybersecurity legislation at national level (11)

Information sharing

Different dynamics:

- Mandatory *Business to Government* notifications of incidents/threats
- Mandatory between interrelated business entities and customers

- Horizontal on peer/local level
  - culture of trust
  - timing is essential

Mandatory via creating information sharing structures on local and peer level (Port Community Systems)?

Accelerating cybersecurity resilience in context MSW

Focus on a cybersecure MSW. How?

1. By stimulating systematic and mandatory attention for cybersecurity in the regular Amendments to FAL (the Annex to the Convention on Facilitation of International Maritime Traffic, 1965 (FAL Convention)).

   Include into Section 1 under *C. Systems for the electronic exchange of information* a new Paragraph*:*

   1.4 *Cybersecurity – Contracting Governments shall safeguard the cybersecurity of entities operating and being connected to the system for the electronic exchange of Information* ***by creating a mandatory framework****.*

2. By being helpful through drafting a Model-law on Cybersecurity.

Concluding Remarks

1. There are many instructive and useful non-mandatory Guidelines and Standards.

2. On top of that we need strong, aligned, and focused mandatory cybersecurity instruments.

3. Accelerate the focus on a cybersecure MSW by including a new *Section 1.4 Cybersecurity* in the Annex to FAL Convention.

4. Be helpful by drafting a Model-Law On Cybersecurity.

iaph

“

Thank you for your attention!

Let’s Stay In Touch!

For your copy of the guidelines:

https://bit.ly/IAPHCyberGuide1

For more information contact:
fransvanzoelen@chello.nl

To join IAPH and its Data Collaboration Committee, contact:

antonis.michail@iaphworldports.org

iaph