Approach Considerations for Developing Sustainable Cybersecurity Capabilities

August 31, 2023

HudsonCyber
Managing Cyber Risk

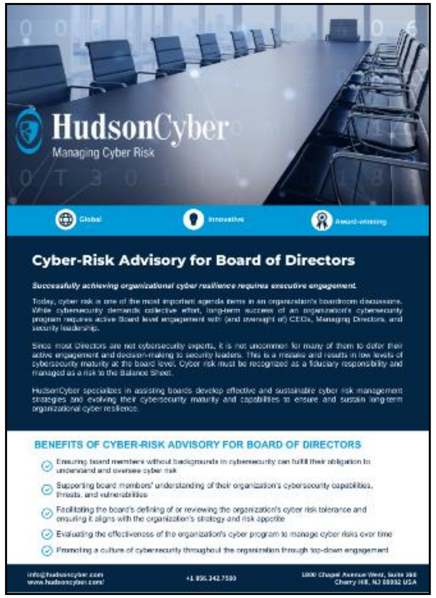
OAS More rights for more people

IPCSA International Port Community Systems Association

CIP Inter-American Committee on Ports

HudsonCyber

Award Winning Cybersecurity Risk Management Solutions



HudsonCyber
Managing Cyber Risk

Global · Innovative · Award-winning

Cyber-Risk Advisory for Board of Directors

Successfully achieving organizational cyber resilience requires executive engagement.

Today, cyber risk is one of the most important agenda items in an organization's boardroom discussions. While cybersecurity demands collective effort, long-term success of an organization's cybersecurity program requires active Board level engagement with (and oversight of) CEOs, Managing Directors, and security leadership.

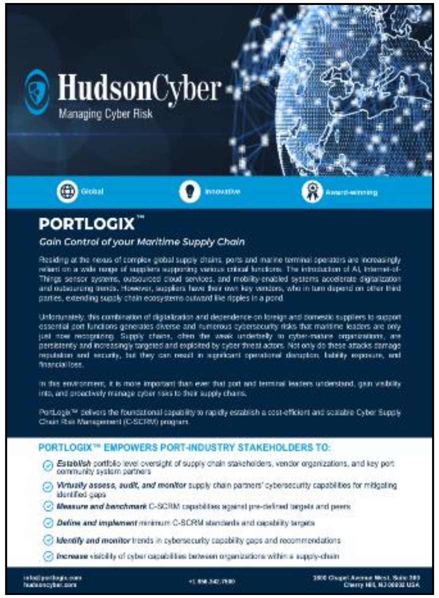
Since most Directors are not cybersecurity experts, it is not uncommon for many of them to defer their active engagement and decision-making to security leaders. This is a mistake and results in low levels of cybersecurity maturity at the board level. Cyber risk must be recognized as a fiduciary responsibility and managed as a risk to the Balance Sheet.

HudsonCyber specializes in assisting boards develop effective and sustainable cyber risk management strategies and evolving their cybersecurity maturity and capabilities to ensure and sustain long-term organizational cyber resilience.

BENEFITS OF CYBER-RISK ADVISORY FOR BOARD OF DIRECTORS

- ✓ Ensuring board members without backgrounds in cybersecurity can fulfill their obligation to understand and oversee cyber risk
- ✓ Supporting board members' understanding of their organization's cybersecurity capabilities, threats, and vulnerabilities
- ✓ Facilitating the board's defining of or reviewing the organization's cyber risk tolerance and ensuring it aligns with the organization's strategy and risk appetite
- ✓ Evaluating the effectiveness of the organization's cyber program to manage cyber risks over time
- ✓ Promoting a culture of cybersecurity throughout the organization through top-down engagement

info@hudsoncyber.com
www.hudsoncyber.com/
+1 856.342.7500
1800 Chapel Avenue West, Suite 360
Cherry Hill, NJ 08002 USA



HudsonCyber
Managing Cyber Risk

Global · Innovative · Award-winning

PORTLOGIX™

Gain Control of your Maritime Supply Chain

Residing at the nexus of complex global supply chains, ports and marine terminal operators are increasingly reliant on a wide range of suppliers supporting various critical functions. The introduction of AI, Internet-of-Things sensor systems, outsourced cloud services, and mobility-enabled systems accelerate digitalization and outsourcing trends. However, suppliers have their own key vendors, who in turn depend on other third parties, extending supply chain ecosystems outward like ripples in a pond.

Unfortunately, this combination of digitalization and dependence on foreign and domestic suppliers to support essential port functions generates diverse and numerous cybersecurity risks that maritime leaders are only just now recognizing. Supply chains, often the weak underbelly to cyber-mature organizations, are persistently and increasingly targeted and exploited by cyber threat actors. Not only do these attacks damage reputation and security, but they can result in significant operational disruption, liability exposure, and financial loss.

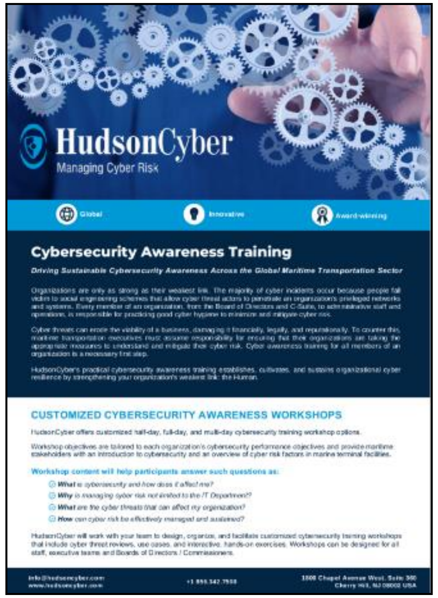
In this environment, it is more important than ever that port and terminal leaders understand, gain visibility into, and proactively manage cyber risks to their supply chains.

PortLogix™ delivers the foundational capability to rapidly establish a cost-efficient and scalable Cyber Supply Chain Risk Management (C-SCRM) program.

PORTLOGIX™ EMPOWERS PORT-INDUSTRY STAKEHOLDERS TO:

- ✓ ***Establish*** portfolio level oversight of supply chain stakeholders, vendor organizations, and key port community system partners
- ✓ ***Virtually assess, audit, and monitor*** supply chain partners' cybersecurity capabilities for mitigating identified gaps
- ✓ ***Measure and benchmark*** C-SCRM capabilities against pre-defined targets and peers
- ✓ ***Define and implement*** minimum C-SCRM standards and capability targets
- ✓ ***Identify and monitor*** trends in cybersecurity capability gaps and recommendations
- ✓ ***Increase*** visibility of cyber capabilities between organizations within a supply-chain

info@portlogix.com
hudsoncyber.com
+1 856.342.7500
1800 Chapel Avenue West, Suite 360
Cherry Hill, NJ 08002 USA



HudsonCyber
Managing Cyber Risk

Global · Innovative · Award-winning

Cybersecurity Awareness Training

Driving Sustainable Cybersecurity Awareness Across the Global Maritime Transportation Sector

Organizations are only as strong as their weakest link. The majority of cyber incidents occur because people fall victim to social engineering schemes that allow cyber threat actors to penetrate an organization's privileged networks and systems. Every member of an organization, from the Board of Directors and C-Suite, to administrative staff and operations, is responsible for practicing good cyber hygiene to minimize and mitigate cyber risk.

Cyber threats can erode the viability of a business, damaging it financially, legally, and reputationally. To counter this, maritime transportation executives must assume responsibility for ensuring that their organizations are taking the appropriate measures to understand and mitigate their cyber risk. Cyber awareness training for all members of an organization is a necessary first step.

HudsonCyber's practical cybersecurity awareness training establishes, cultivates, and sustains organizational cyber resilience by strengthening your organization's weakest link: the Human.

CUSTOMIZED CYBERSECURITY AWARENESS WORKSHOPS

HudsonCyber offers customized half-day, full-day, and multi-day cybersecurity training workshop options.

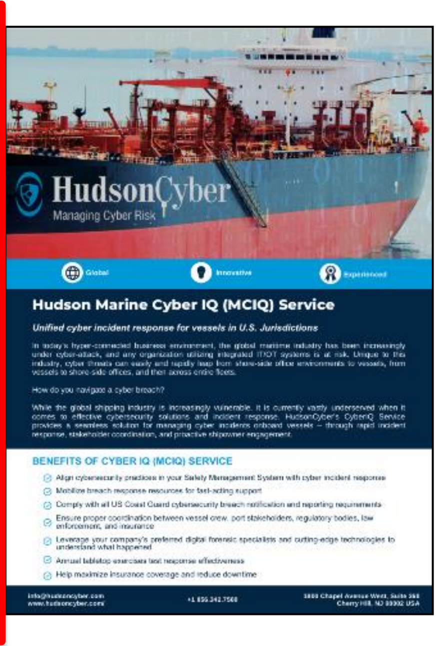
Workshop objectives are tailored to each organization's cybersecurity performance objectives and provide maritime stakeholders with an introduction to cybersecurity and an overview of cyber risk factors in marine terminal facilities.

Workshop content will help participants answer such questions as:

- ***What*** *is cybersecurity and how does it affect me?*
- ***Why*** *is managing cyber risk not limited to the IT Department?*
- ***What*** *are the cyber threats that can affect my organization?*
- ***How*** *can cyber risk be effectively managed and sustained?*

HudsonCyber will work with your team to design, organize, and facilitate customized cybersecurity training workshops that include cyber threat reviews, use cases, and interactive, hands-on exercises. Workshops can be designed for all staff, executive teams and Boards of Directors / Commissioners.

info@hudsoncyber.com
www.hudsoncyber.com
+1 856.342.7500
1800 Chapel Avenue West, Suite 360
Cherry Hill, NJ 08002 USA



HudsonCyber
Managing Cyber Risk

Global · Innovative · Experienced

Hudson Marine Cyber IQ (MCIQ) Service

Unified cyber incident response for vessels in U.S. Jurisdictions

In today's hyper-connected business environment, the global maritime industry has been increasingly under cyber-attack, and any organization utilizing integrated IT/OT systems is at risk. Unique to this industry, cyber threats can easily and rapidly leap from shore-side office environments to vessels, from vessels to shore-side offices, and then across entire fleets.

How do you navigate a cyber breach?

While the global shipping industry is increasingly vulnerable, it is currently vastly underserved when it comes to effective cybersecurity solutions and incident response. HudsonCyber's CyberIQ Service provides a seamless solution for managing cyber incidents onboard vessels – through rapid incident response, stakeholder coordination, and proactive shipowner engagement.

BENEFITS OF CYBER IQ (MCIQ) SERVICE

- ✓ Align cybersecurity practices in your Safety Management System with cyber incident response
- ✓ Mobilize breach response resources for fast-acting support
- ✓ Comply with all US Coast Guard cybersecurity breach notification and reporting requirements
- ✓ Ensure proper coordination between vessel crew, port stakeholders, regulatory bodies, law enforcement, and insurance
- ✓ Leverage your company's preferred digital forensic specialists and cutting-edge technologies to understand what happened
- ✓ Annual tabletop exercises test response effectiveness
- ✓ Help maximize insurance coverage and reduce downtime

info@hudsoncyber.com
www.hudsoncyber.com/
+1 856.342.7500
1800 Chapel Avenue West, Suite 360
Cherry Hill, NJ 08002 USA

CIP Inter-American Committee on Ports
enisa European Union Agency for Cybersecurity
AAPA Essential. Resilient. United. Seaports Deliver
IAPH International Association of Ports and Harbors
CSA Caribbean Shipping Association
S&P Global Ratings
Maritime Protection Group
AON Empower Results®
Steamship Mutual
Chaucer Cyber
MITRE
Shoreline
SC CapRock
Transportation System Information Sharing and Analysis Center

Primary cybersecurity services:

- Cybersecurity advisory and risk management
- Tailored threat intelligence
- Custom training solutions

HudsonCyber: What we’ve done

At the forefront of driving cyber risk management best practices and international standards in the global maritime industry.

Global service built around you

North

IN PARTNERSHIP WITH

HudsonCyber
Managing Cyber Risk

Cyber Security Kick Start

Preparing for Cyber Security Compliance - FAQs

North P&I Club has partnered with HudsonCyber to offer Members free access to their HACyberLogix assessment tool.

Q Why Act Now?

A The International Maritime Organization (IMO) has stated that cyber security on vessels must be included in the safety management system (SMS) from January 2021. It is important to plan the changes well in advance of the 2021 deadline. The changes required may be both time-consuming and complex. This initiative will help North's Members meet their regulatory obligations and reduce cyber risk across their operations.

Q What is HACyberLogix?

A HACyberLogix is a secure, cloud-based program designed specifically for the global shipping industry. It allows shipping companies to:

1. Assess their organisation's cyber security capabilities.
2. Identify cyber security vulnerabilities.
3. Receive specific guidance for supporting the implementation, continuous improvement, and long-term sustainability of a cyber security program supporting all shore-based and shipboard operating environments.

By taking a maturity model approach, HACyberLogix will enable North's Members to assess and benchmark their cyber security practices.

Q Will it help achieve IMO 2021 compliance?

A Yes. The HACyberLogix methodology integrates industry-leading cyber security standards, frameworks, and standardised practices with key elements of the International Maritime Organization's (IMO) International Ship and Port Security Code and the International Safety Management Code.

HACyberLogix empowers decision-makers to rapidly and cost-effectively implement and sustain a cyber risk management framework compliant with the IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). It also positions them to comply with Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems, which affirms incorporating cyber risk management efforts into approved Safety Management Systems in accordance with the objectives and requirements of the ISM Code.

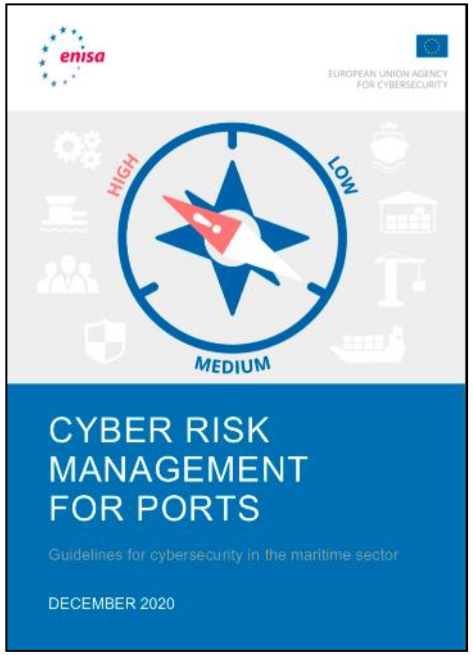
HACYBERLOGIX METHODOLOGY INTEGRATES:

NIST | ISO 27001 | ISPS CODE | ISM CODE | CIS CRITICAL CONTROLS

For more information, please visit www.nepia.com

Copyright © 2020 The North of England P&I Association Limited

Sept – Oct 2020



enisa

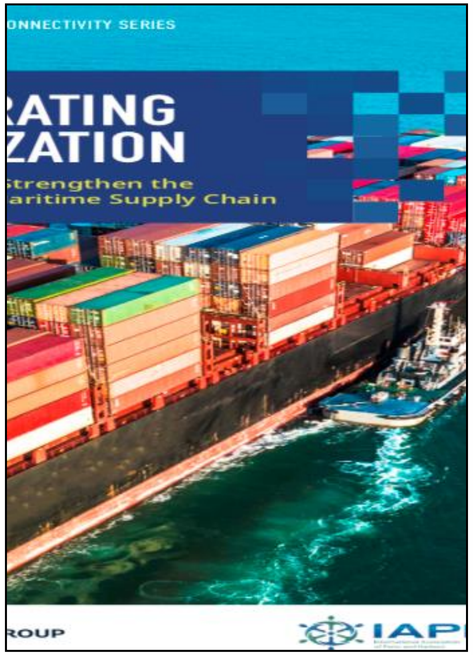
EUROPEAN UNION AGENCY FOR CYBERSECURITY

CYBER RISK MANAGEMENT FOR PORTS

Guidelines for cybersecurity in the maritime sector

DECEMBER 2020

December 2020



ONNECTIVITY SERIES

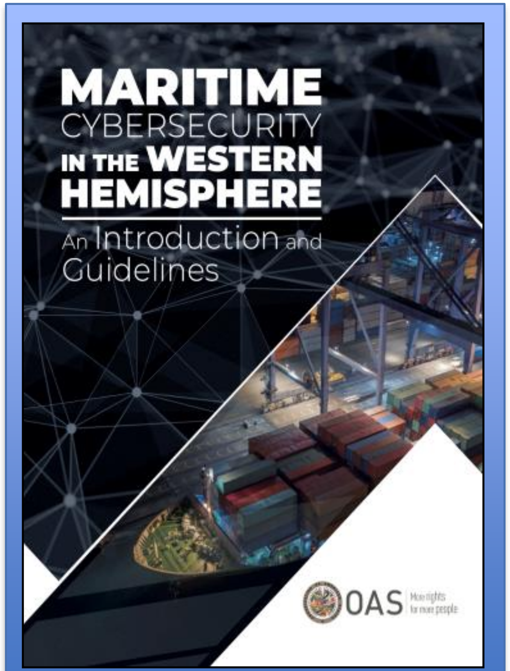
RATING
ZATION

Strengthen the
aritime Supply Chain

ROUP

IAP

January 2021

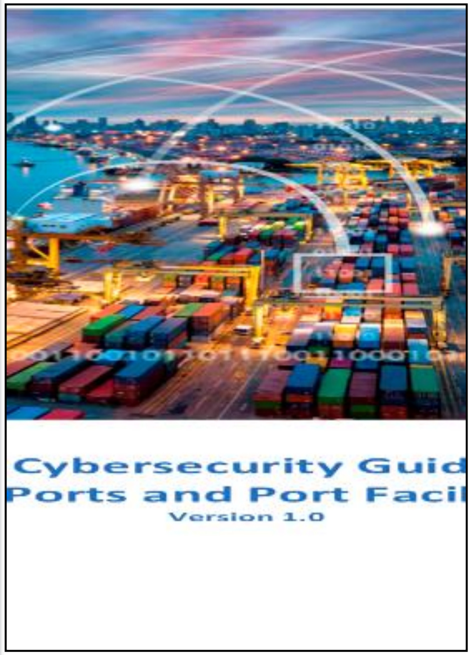


MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

OAS More rights for more people

May 2021



Cybersecurity Guid
Ports and Port Facil
Version 1.0

September 2021

Cybersecurity Challenges

The cyber battlefield

Evolving pressures

Ransomware attack on maritime soft
impacts 1,000 ships
vessels have been affected by a ran

Increasing threat activity targeting the maritime sector

Increasing digitalization efforts expanding the attack surface

Limited Understanding in C-Suite / Board Level

Lack of maritime-specific cybersecurity subject matter expertise

Increasing responsibility through regulations and oversight

Multiple requirements and evolving pressures.

Threats: Internal

Lack of cybersecurity subject matter expertise across C-Suite

Rationale often presented for inaction:

- ***Cybersecurity is too expensive*** **–** There is no budget. Misperception of only technical solutions
- ***The competitive imperative*** – Trade offs are frequently made between security and operations
- ***Cyber risk is pervasive*** – It is often perceived of as something that is overwhelming
- ***Cyber risk is difficult to quantify*** – No common tools exist to help business leaders understand exposure.
- ***Difficult to change behavior*** – Nothing's happened, so why change?

What is the impact of digitalization? What's vulnerable?

- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) for loading / unloading of bulk / containerized cargo
- Cargo / Terminal Operating Systems
- Security Domain Awareness – RADAR, AIS, VTS/VTMS, GIS Systems
- *Any* Business Software Application (e.g., email, financial,

  human resources, finance, logistics, business operations
- *Any* Operating System (e.g., Microsoft, Linux)
- *Any* Security System – CCTV, PACS, etc.
- *Any* Mobility device and platform (RFID)
- Communications Systems
- Employees (insiders) and Contractors
- You!

High-Probably Compromise: ERP Systems

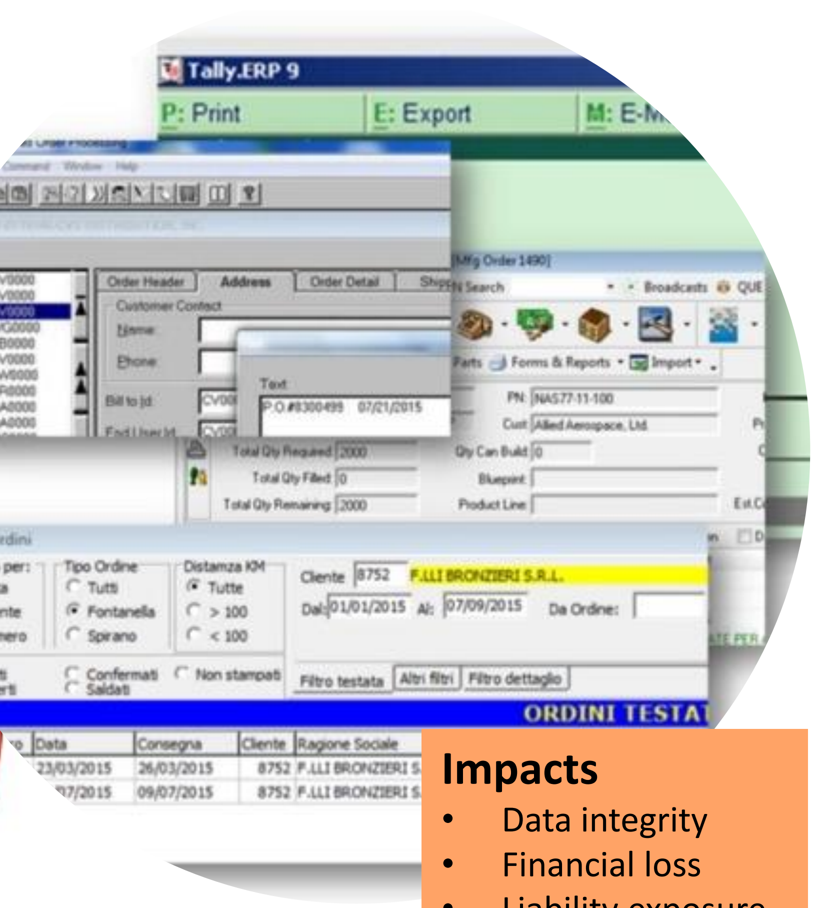
Enterprise Resource Planning (ERP) Systems offer virtual windows into an organization’s activities as it relates to *people, resources, goods,* and *money*.

ERP Systems *integrate core business processes* and leverage shared databases to support multiple functions used by different business units.

Systems affected include:

- Port Community System Applications
- Financial (re: Fraud, Payment info)
- Cargo Handling & Management
- Taxes (e.g., VAT)
- Customs
- Banking
- Shipping

FINANCE ACCOUNTING
%
HUMAN RESOURCES
ACCESS CONTROL
ERP
Enterprise Resource Planning
PURCHASING
$
CRM
DATA SERVICES
PROJECT MANAGEMENT



Text P.O.#8300499 07/21/2015

Total Qty Required 2000
Total Qty Filled 0
Total Qty Remaining 2000

PN NAS77-11-100
Cust Allied Aerospace, Ltd
Qty Can Build 0

Cliente 8752 F.LLI BRONZIERI S.R.L.
Dal: 01/01/2015 Al: 07/09/2015 Da Ordine:

Data	Consegna	Cliente	Ragione Sociale
23/03/2015	26/03/2015	8752	F.LLI BRONZIERI S
07/2015	09/07/2015	8752	F.LLI BRONZIERI S

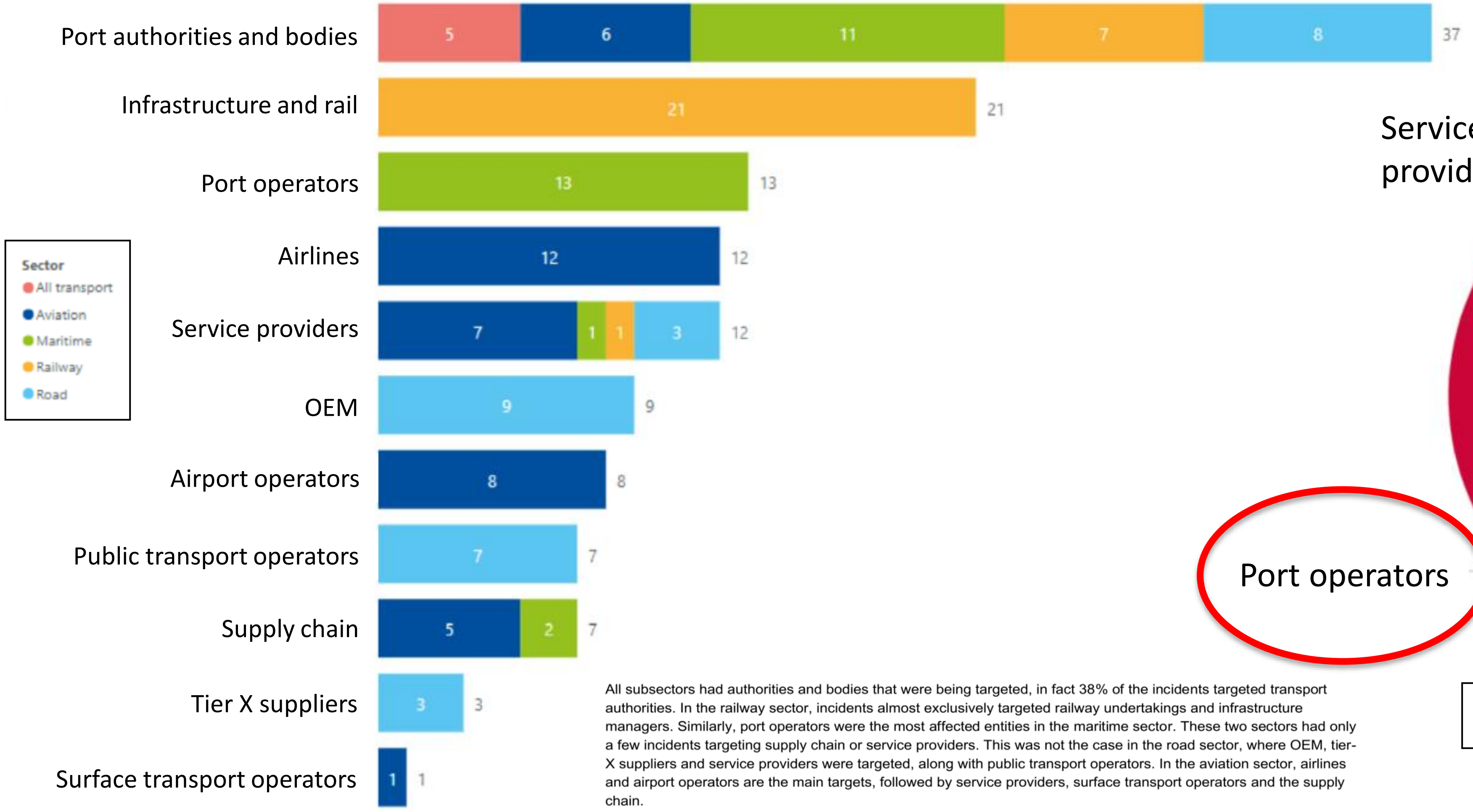
Impacts

- Data integrity
- Financial loss
- Liability exposure
- Operational delays

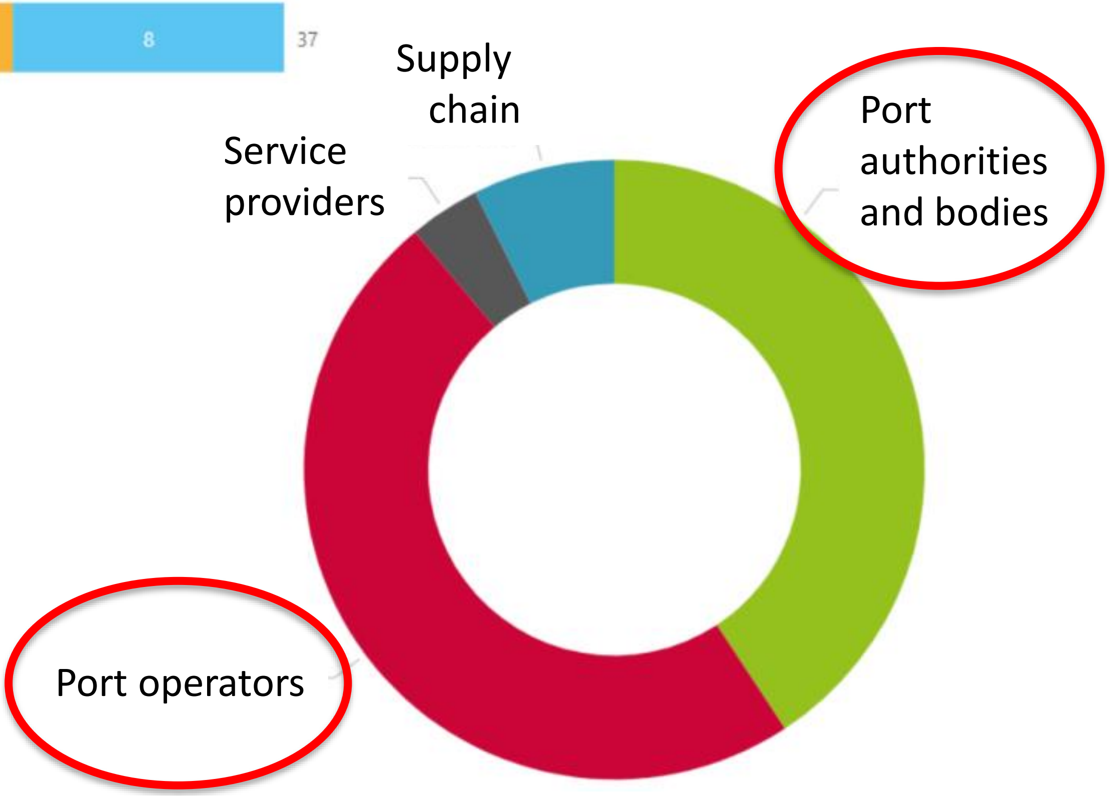
Targets:
Port Authorities and terminal operators most at risk

**ENISA Threat Landscape: Transport Sector* (Jan 2021-Oct 2022); Published March 2023

Transportation Sector Comparison



All subsectors had authorities and bodies that were being targeted, in fact 38% of the incidents targeted transport authorities. In the railway sector, incidents almost exclusively targeted railway undertakings and infrastructure managers. Similarly, port operators were the most affected entities in the maritime sector. These two sectors had only a few incidents targeting supply chain or service providers. This was not the case in the road sector, where OEM, tier-X suppliers and service providers were targeted, along with public transport operators. In the aviation sector, airlines and airport operators are the main targets, followed by service providers, surface transport operators and the supply chain.



Maritime Target Distribution

Steps for Developing Organizational Cybersecurity Capabilities

Initial steps for developing organizational cybersecurity capabilities

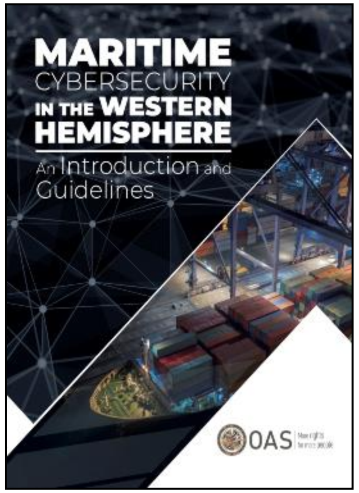
Step 1. **Identify who is responsible within the organization for overseeing all cyber risk management and cybersecurity activities (REF: 4.1).**

Step 2. **Define the internal personnel and external parties who are involved in the organization's cybersecurity activities (REF: 4.2).**

Step 3. **Create a steering committee to formally coordinate and manage all cyber risk management initiatives (REF: 4.3)**

Step 4. **Perform a baseline assessment of the organization's overall cybersecurity capabilities (REF: 4.4)**

Step 5. **Implement a cyber risk management strategy and plan (REF: 4.5)**



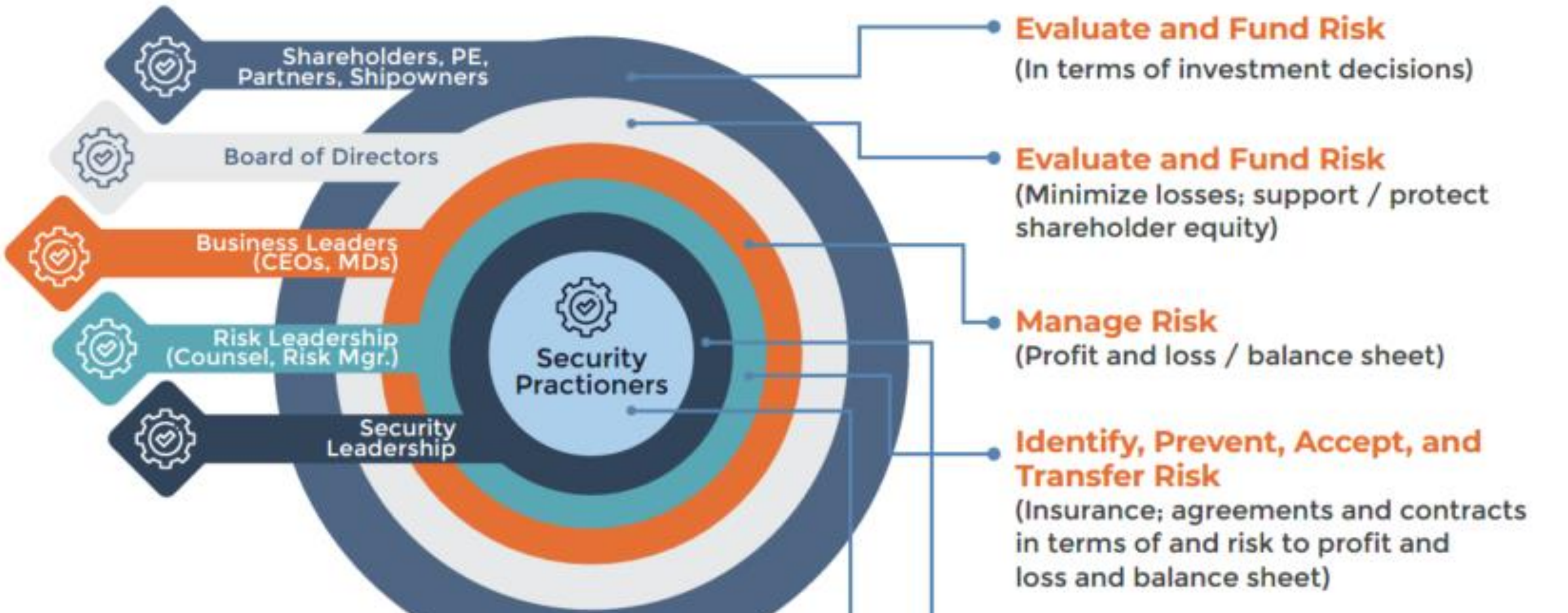
MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE

An Introduction and Guidelines

OAS

HudsonCyber
Maritime Cyber Security

Foundational considerations for the cyber steering committee


Shareholders, PE, Partners, Shipowners
Board of Directors
Business Leaders (CEOs, MDs)
Risk Leadership (Counsel, Risk Mgr.)
Security Leadership
Security Practioners

Evaluate and Fund Risk
(In terms of investment decisions)

Evaluate and Fund Risk
(Minimize losses; support / protect shareholder equity)

Manage Risk
(Profit and loss / balance sheet)

Identify, Prevent, Accept, and Transfer Risk
(Insurance; agreements and contracts in terms of and risk to profit and loss and balance sheet)

Validate Risk, Allocate Resources
(In terms of cyber risk to operations and profit and loss)

Communicate Needs, Solutions
(In terms of cyber risk to operations that supports cash flow and profit and loss)

Foundational consideration for driving change:

Redefine cyber risk management as a money discussion

- ✓ Consider cyber risk in terms of ***money***
- ✓ *The **cyber-risk-to-money intersection** offers measurable value to support resource allocation and prioritization*
- ✓ Financial “grounding” translates cyber risk into a common language
- ✓ Empowers decision-makers with context to make informed decisions on cyber risk

Foundational considerations for cyber resilience:
Establishing and sustaining the cyber-risk-to-money intersection

Develop the business case

Determine business impact

- Identify critical assets, systems, equipment, and infrastructure
- Characterize impact– income, health and safety, environment, reputation, etc.

Develop and apply realistic loss scenarios

- Engage all relevant stakeholders
- Develop and agree on scope, probability, realism, context
- Determine financial value-at-risk

Enable organizational resilience

Leverage a common vocabulary

- Institute a common vocabulary with clear definitions
- Assign financial values to top 5 scenarios

Establish the cyber-risk-to-money intersection

- Dedicate a cybersecurity budget
- Prioritize budget allocations based on criticality
- Test incident response (and cyber insurance) against loss scenarios

Case Study: Barbados Port Inc. PCS (2022)

OAS CIP Maritime Award of the Americas for Cybersecurity

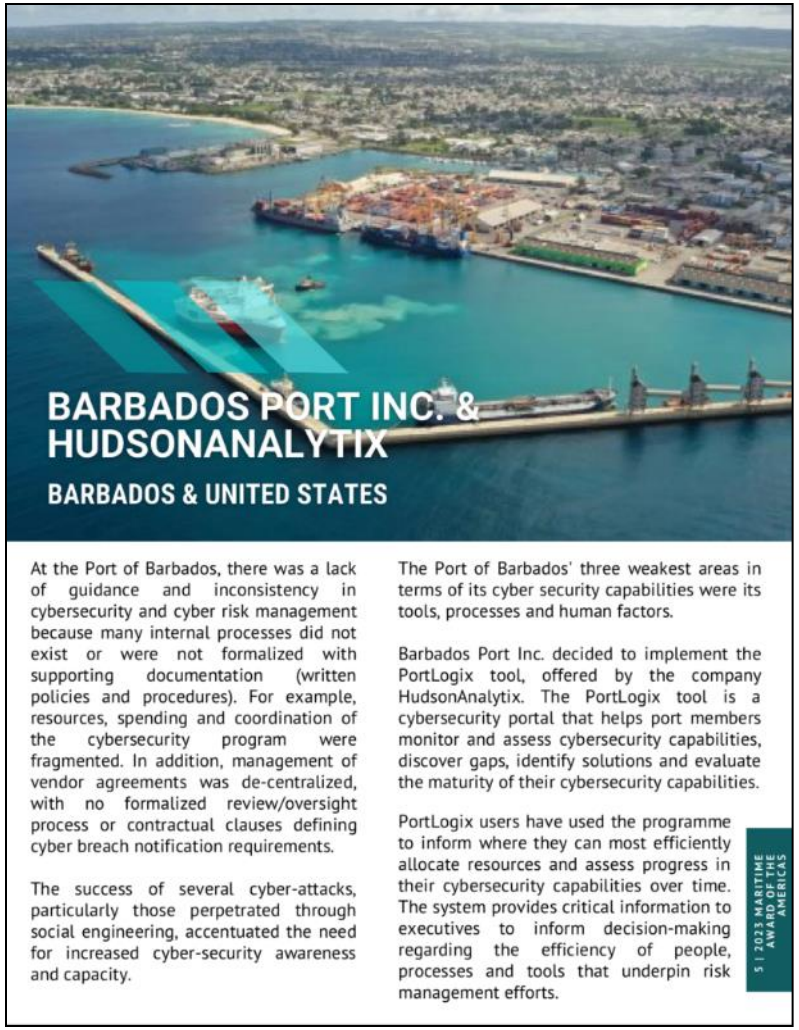
ORGANIZATION OF AMERICAN STATES
OAS
More rights for more people

BARBADOS
PORT INC.

CARIBBEAN DEVELOPMENT BANK

WINNING PRACTICES
Maritime Award of the Americas
2023
"Integral Management for Port Sector Modernization in the Americas"

OAS More rights for more people
CIP Inter-American Committee on Ports
OAS CIM
NAMEPA
SLOM



BARBADOS PORT INC. & HUDSONANALYTIX

BARBADOS & UNITED STATES

At the Port of Barbados, there was a lack of guidance and inconsistency in cybersecurity and cyber risk management because many internal processes did not exist or were not formalized with supporting documentation (written policies and procedures). For example, resources, spending and coordination of the cybersecurity program were fragmented. In addition, management of vendor agreements was de-centralized, with no formalized review/oversight process or contractual clauses defining cyber breach notification requirements.

The success of several cyber-attacks, particularly those perpetrated through social engineering, accentuated the need for increased cyber-security awareness and capacity.

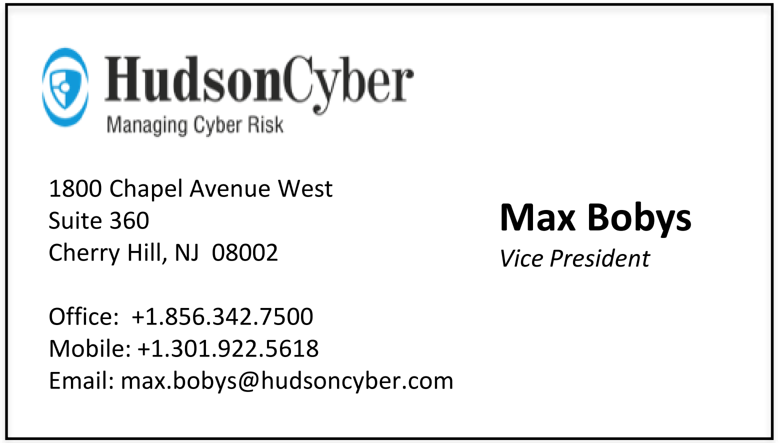
The Port of Barbados' three weakest areas in terms of its cyber security capabilities were its tools, processes and human factors.

Barbados Port Inc. decided to implement the PortLogix tool, offered by the company HudsonAnalytix. The PortLogix tool is a cybersecurity portal that helps port members monitor and assess cybersecurity capabilities, discover gaps, identify solutions and evaluate the maturity of their cybersecurity capabilities.

PortLogix users have used the programme to inform where they can most efficiently allocate resources and assess progress in their cybersecurity capabilities over time. The system provides critical information to executives to inform decision-making regarding the efficiency of people, processes and tools that underpin risk management efforts.

5 | 2023 MARITIME AWARD OF THE AMERICAS

Thank You



HudsonCyber
Managing Cyber Risk

1800 Chapel Avenue West
Suite 360
Cherry Hill, NJ 08002

Office: +1.856.342.7500
Mobile: +1.301.922.5618
Email: max.bobys@hudsoncyber.com

Max Bobys
Vice President

www.hudsoncyber.com