Mobility and Transport Connectivity Series

WORLD BANK GROUP

Cybersecurity in Ports: Shifting from Risk to Resilience

Dominik Englert, Senior Economist,
World Bank Group

Thursday, 21st May 2026

QUALITY INFRASTRUCTURE INVESTMENT PARTNERSHIP

Cybersecurity MULTI-DONOR TRUST FUND

Key Findings

01

Cybersecurity is a **critical building block** for making ports more **resilient** and enabling economic development.

02

Significant gaps exist between **high-income** and **low- and middle-income countries** in their capacity to deal with cyber risks—but no port ecosystem appears fully prepared yet.

03

Overcoming policy, process, and capacity **constraints** to cybersecurity in ports can unlock more efficient, safer, and more resilient port operations.

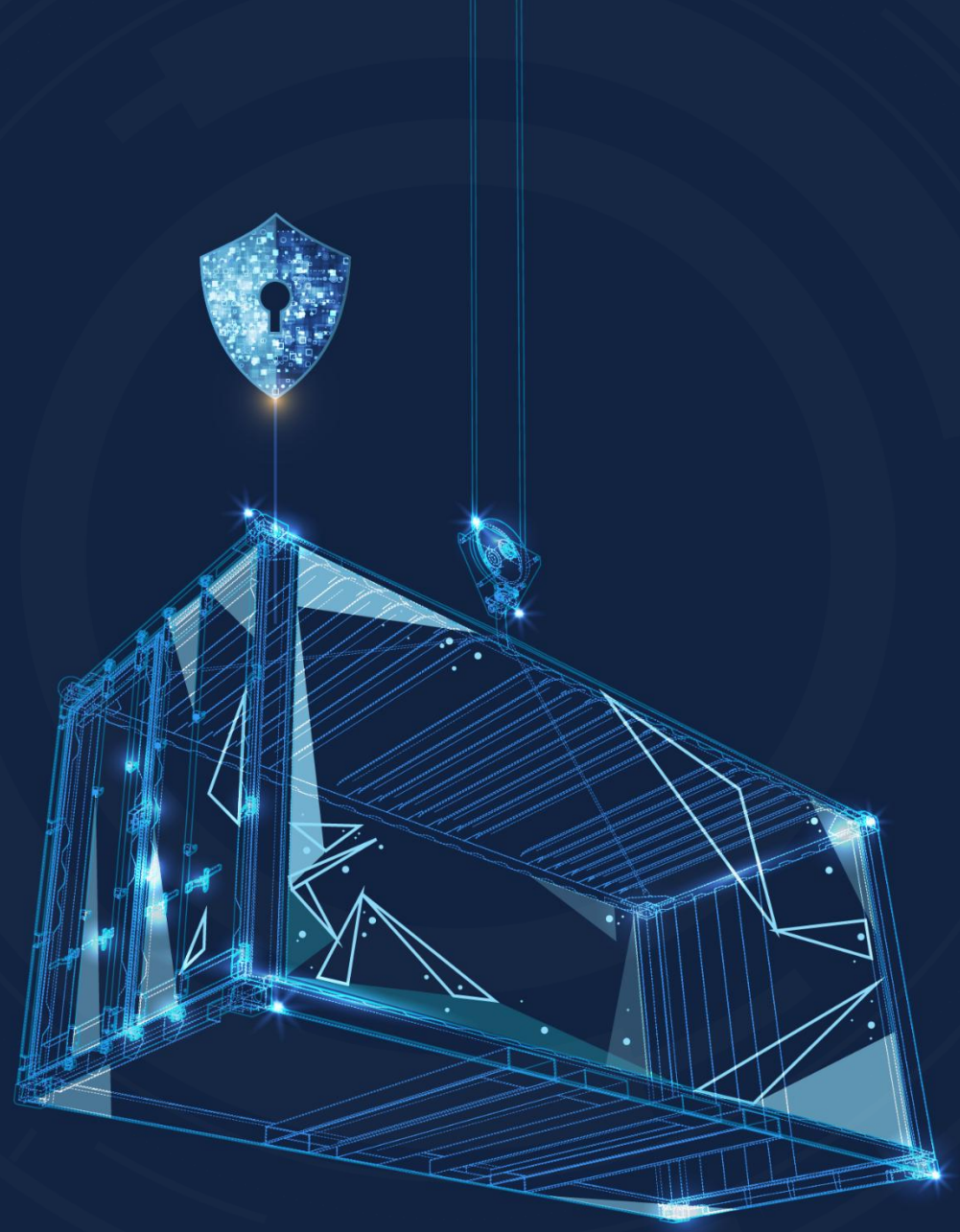
Agenda

01 Overview of the Report

02 Importance of Cybersecurity in Ports

03 Gaps in Cyber Resilience of Ports

04 Recommendations

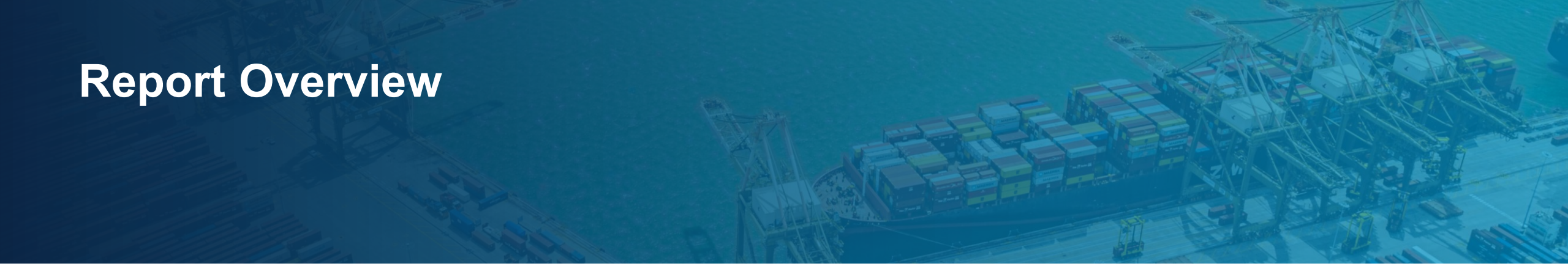


01

Overview of Report

WORLD BANK GROUP

Report Overview



Unique dataset

- A **global survey** of 109 port stakeholders
- In-depth interviews
- Literature review
- Consultations with and reviews by peers

Current Landscape Overview

- Focus on **low- and middle-income countries (LMICs)**
- Framing around 3 key areas: Policy, Practice, Barriers
- Case studies to highlight best practices

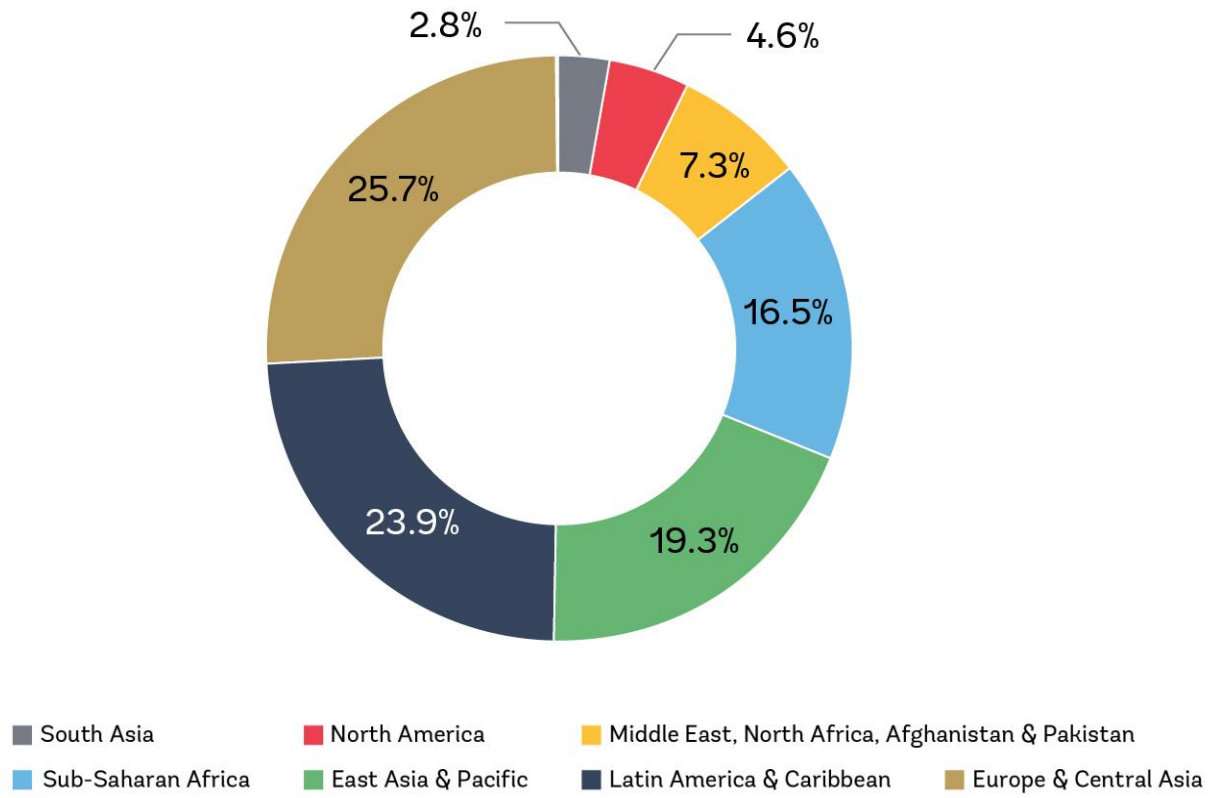
Actionable Recommendations

- Aimed at policymakers, port authorities, operators and development partners
- Technology agnostic
- Moving from a reactive to a **proactive approach**

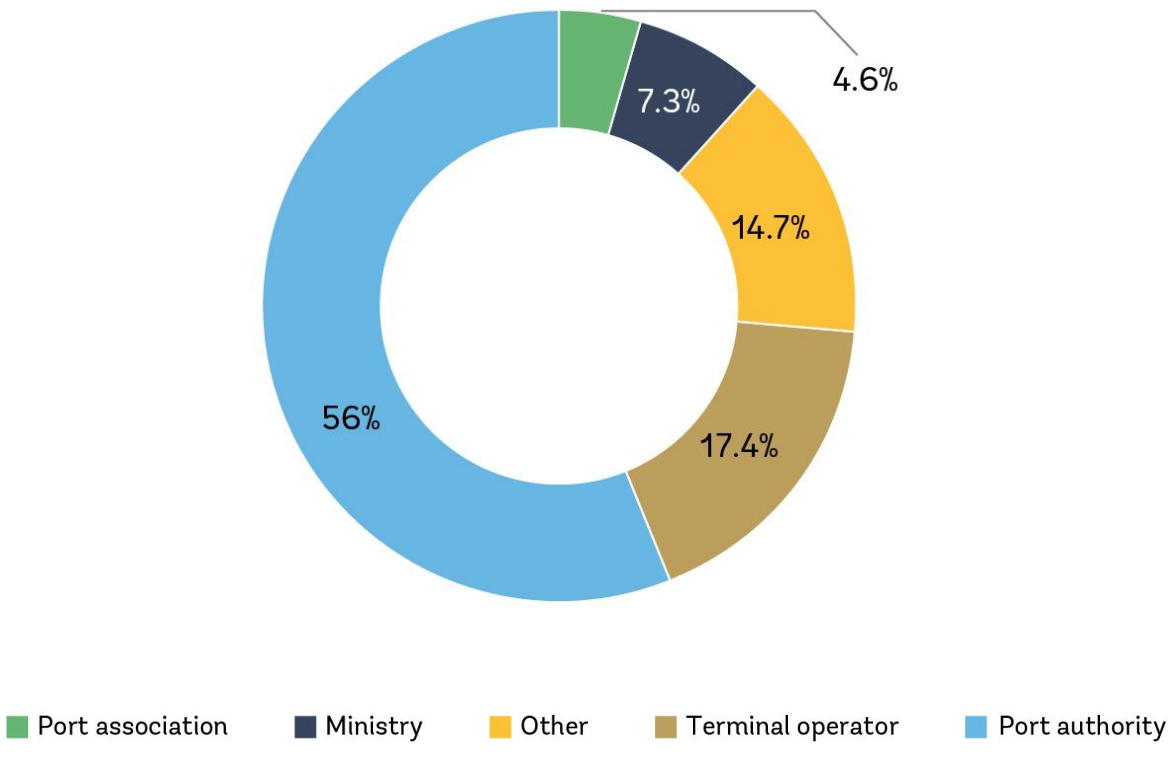
Survey Respondents

Autumn 2025 Survey

Geography



Organizational Type



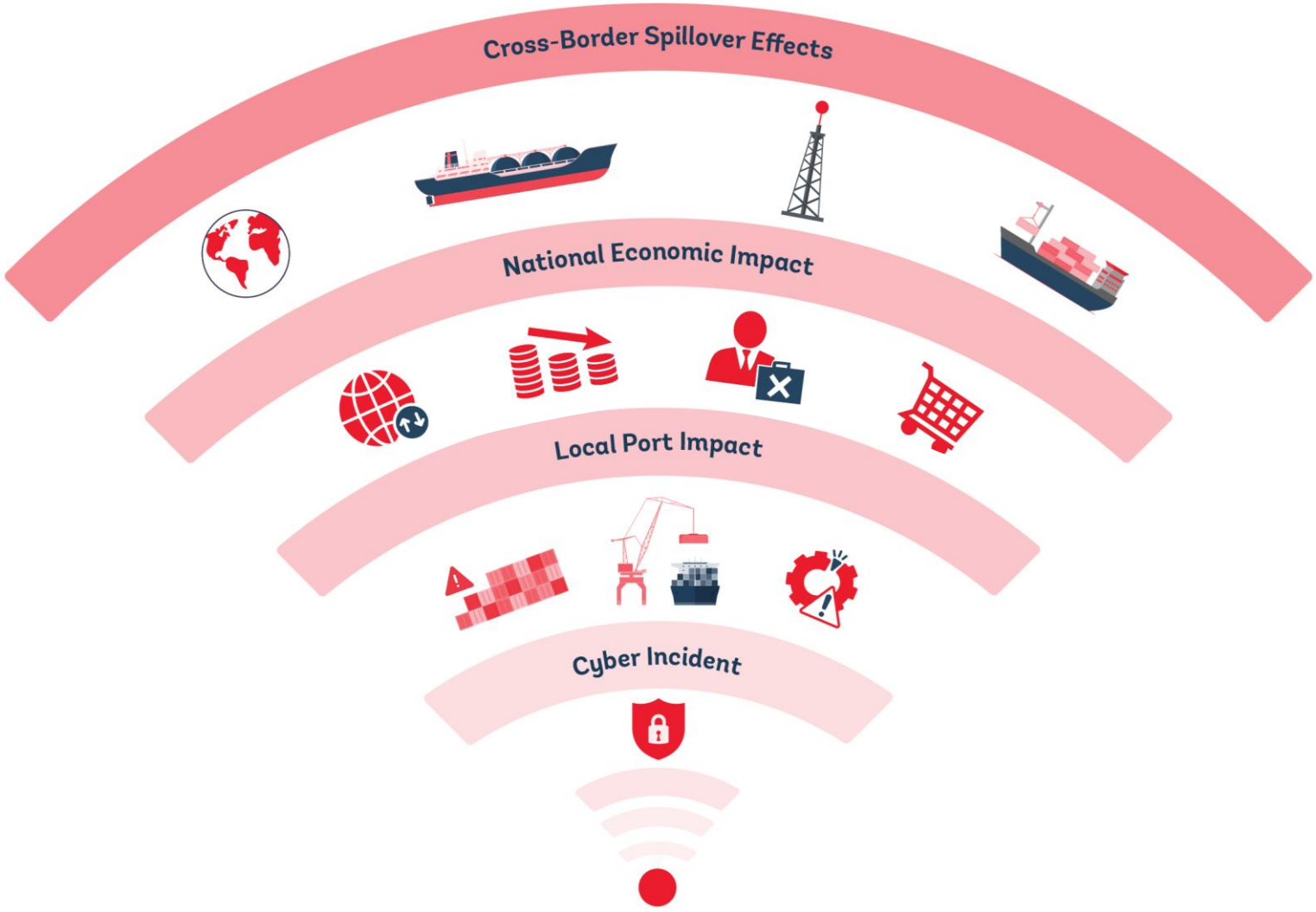
02

Importance of Cybersecurity in Ports

WORLD BANK GROUP

Why does cybersecurity in ports matter?

- Digitalization improves efficiency & transparency
- It also leads to greater cyber risk exposure
- An incident can have financial impacts, cause physical damage, loss of trust, and lead to wider trade flow disruption
- Cybersecurity represents a critical building block for making ports more resilient and for enabling economic development.



WORLD BANK GROUP

Impacts of Cyber Incidents

Operations

- Operations systems and websites **damaged**
- **Stranded** cargo and **disrupted** Just-in-Time supply chains
- **Closed** or **disrupted** terminals

Direct Costs

- Average **cyber incident** in maritime cost $550,000*
- **Ransom demands** averaged $3.2 million*
- Average **cost of data breach** across critical infrastructure in 2024 was $4.88 million**

** Industry estimate, Kenney & Macdonald (2023). ** IBM (2022).*

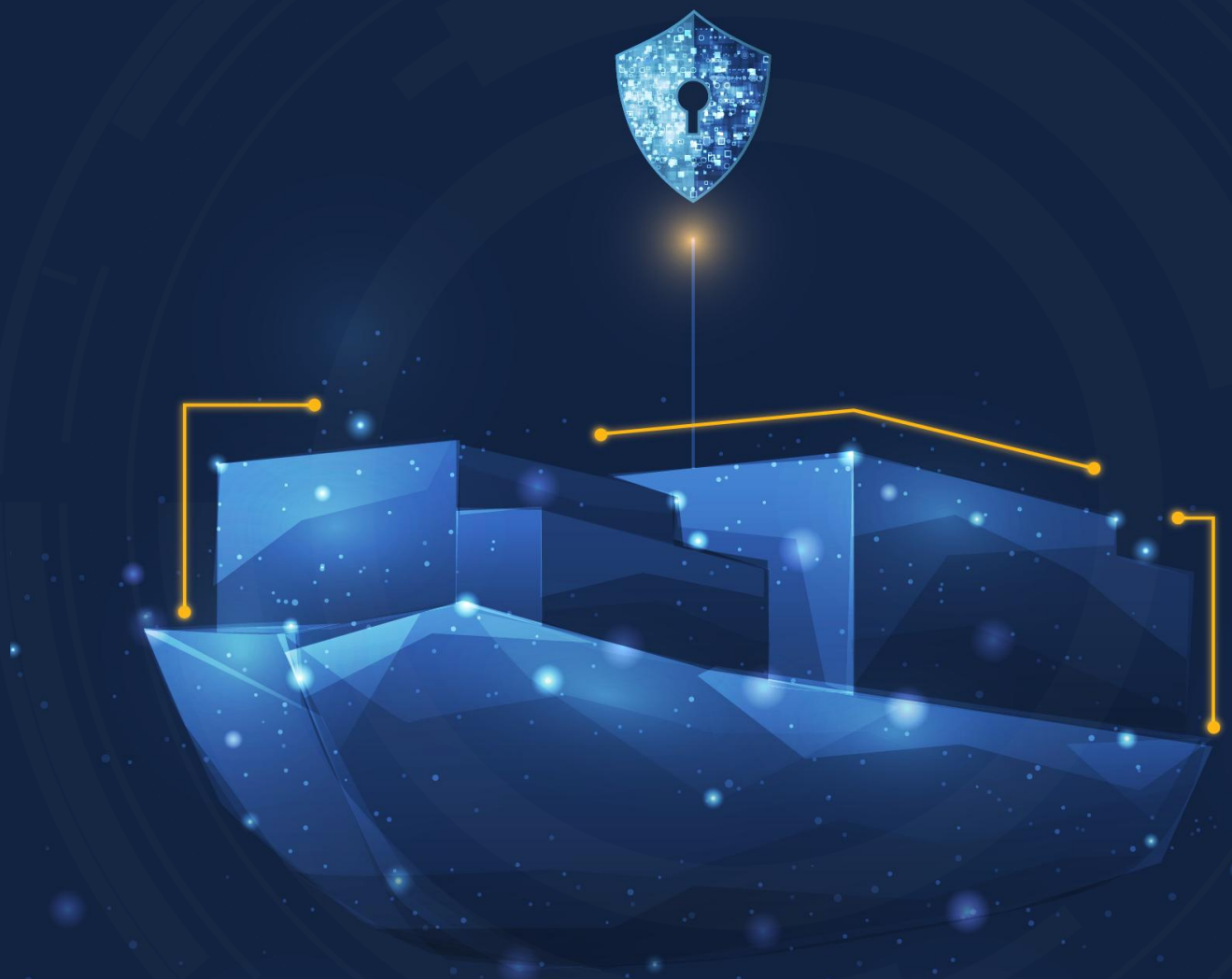
Indirect Costs

- Supply chain disruptions – estimated $7.3 bn cost of **Maersk NotPetya** incident*
- Reducing cyber incidents could **increase GDP** per capita by 1.5%**

** Badea et al. (2025), Steinberg et al. (2021). ** Vergara Cobos (2024).*

03

Gaps in Cyber Resilience of Ports



WORLD BANK GROUP

Gaps in Cyber Resilience are Universal

01

Significant gaps exist between high-income and low- and middle-income countries in their capacity to deal with cyber risks.

However, **no port ecosystem** appears **fully prepared.**

02

Countries show, among others:

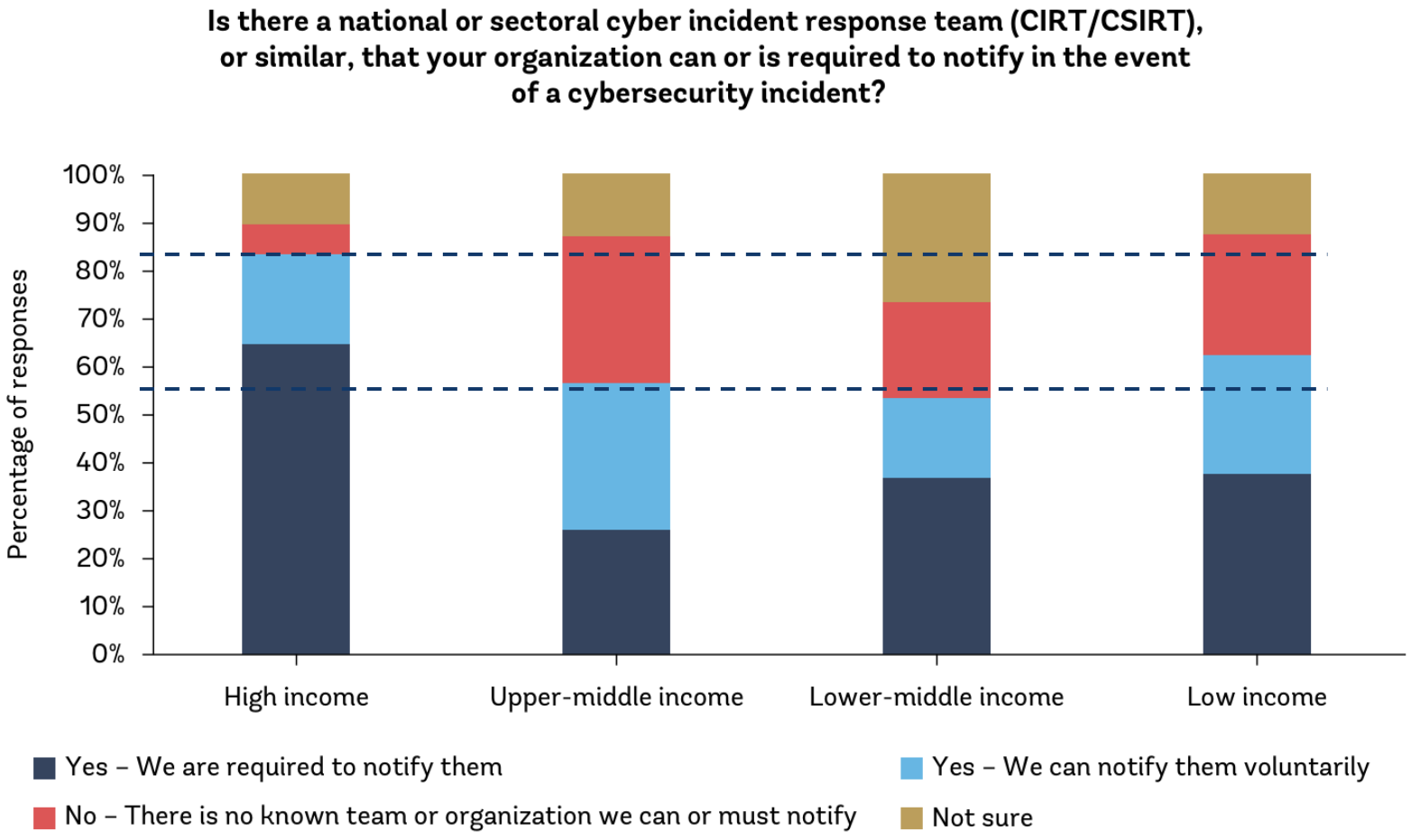
- Uneven **compliance** with cybersecurity frameworks
- Inconsistent risk assessments
- Inadequate incident preparedness

03

Challenges are **more pronounced in LMICs** due to:

- Thinner provisions on national and sectoral **policy frameworks**
- Wider **skills gaps**
- Constrained financial and human **resources**

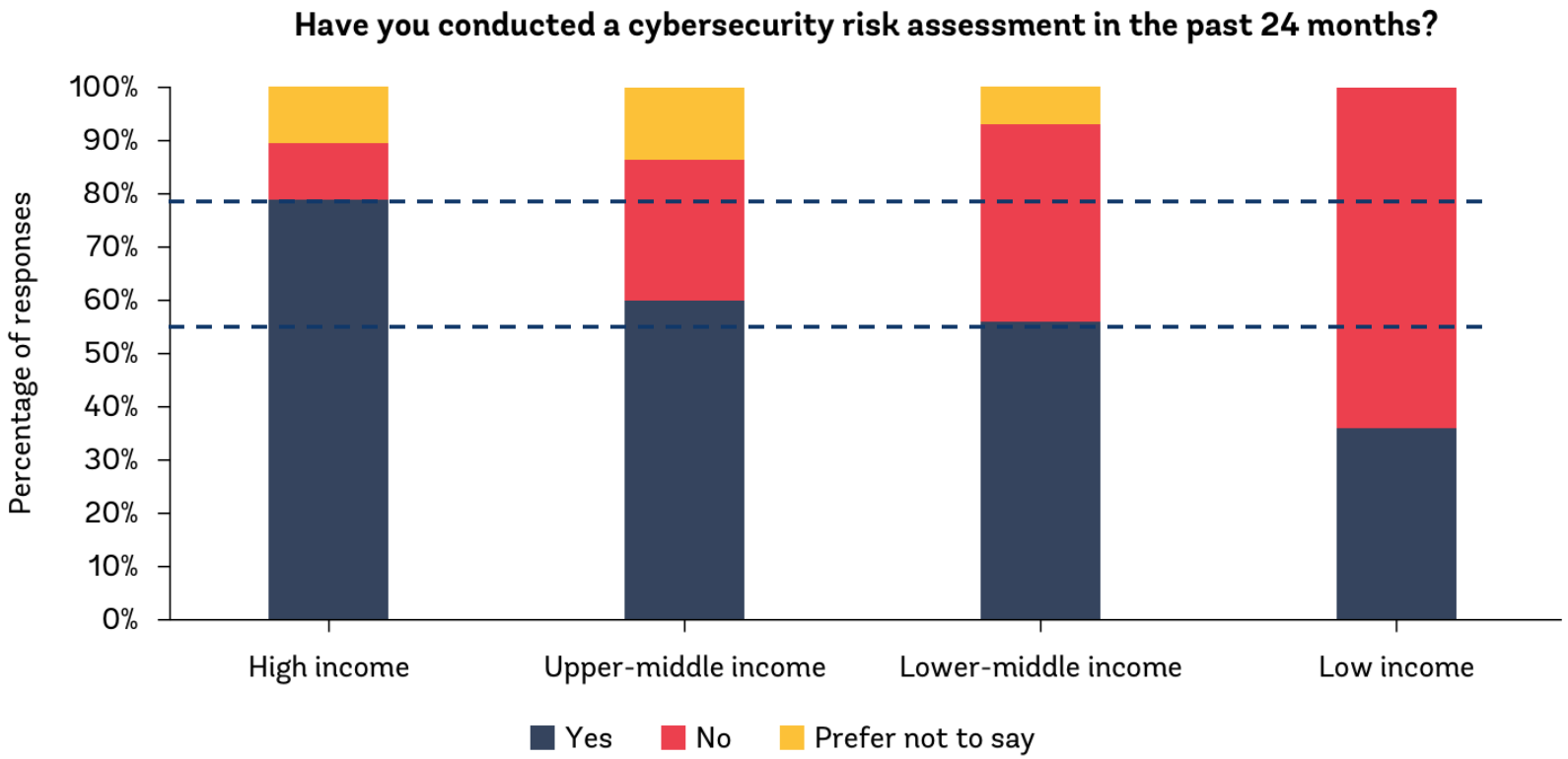
Policy: Dealing with uneven requirements



- No binding global framework for port cybersecurity
- Only half of countries worldwide have cybersecurity legislation applicable to infrastructure critical to national economies
- Less than half of surveyed comply with existing frameworks
- 83% of surveyed in high-income countries report incidents vs. 56% in LMICs

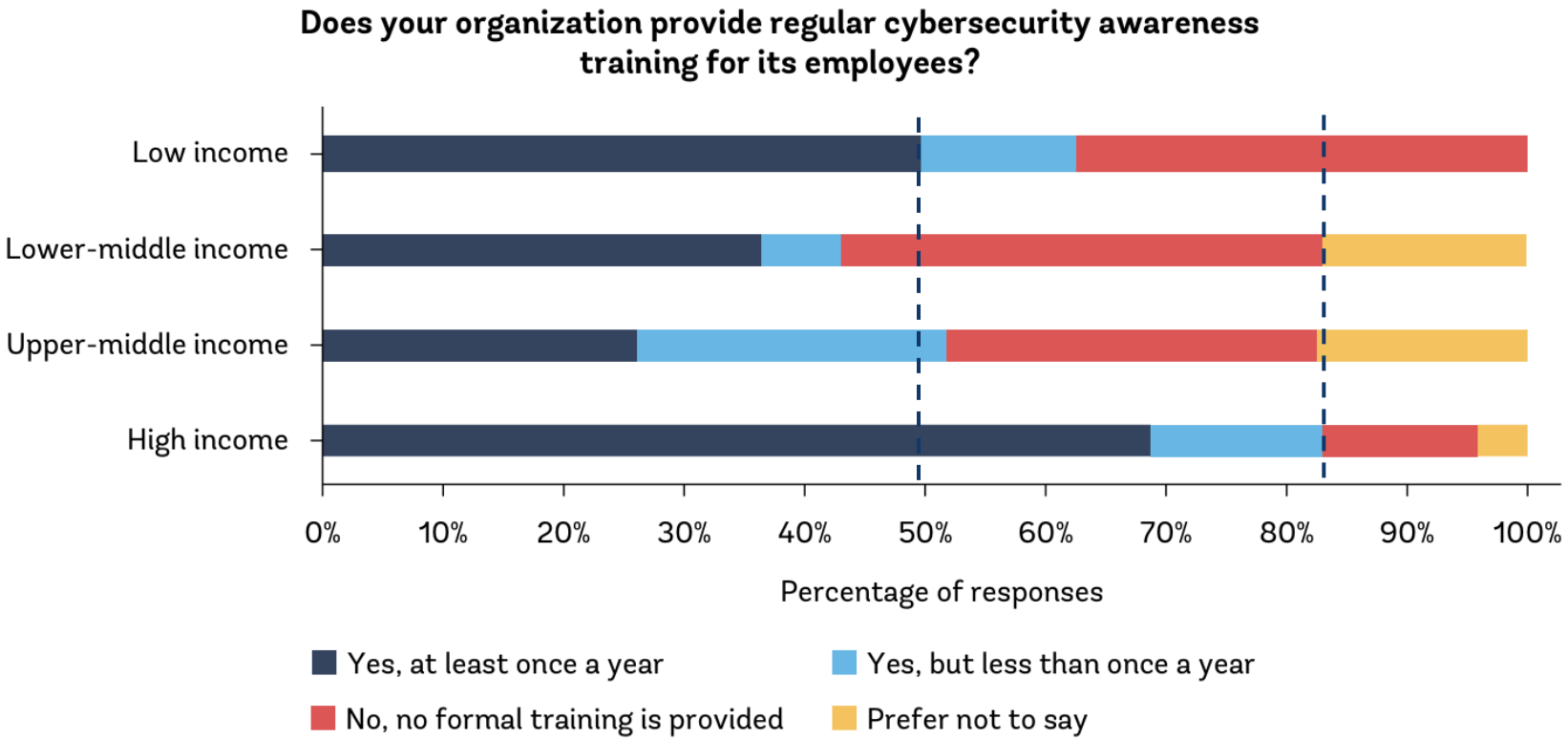
WORLD BANK GROUP

Practice: Adopting a Proactive Approach



- A reactive approach remains more common than a proactive approach
- Risk assessments are a basic component of cybersecurity
- In high-income countries, 79% of respondents conducted a cybersecurity risk assessment in the past 2 years. In LMICs, this decreases to 56%.
- Cybersecurity appears integrated into business continuity planning far more consistently in high-income countries than in LMICs

Barriers: Enhancing skills and capacities



- Human, financial, and economic barriers continue to limit progress towards cyber resilient supply chains
- 84% of high-income country respondents vs. 49% of LMIC country respondents provide regular cybersecurity training
- Cybersecurity averts losses rather than generating revenues
- Unclear responsibilities, information gaps, and free riding weaken incentives to invest
- Lack of voluntary information sharing

04

Recommendations

Overcoming the Global Port Cyber Resilience Gap

Strengthen Policy

- Binding **cyber rules**
- Clear **responsibilities**
- Mandatory **incident reporting**

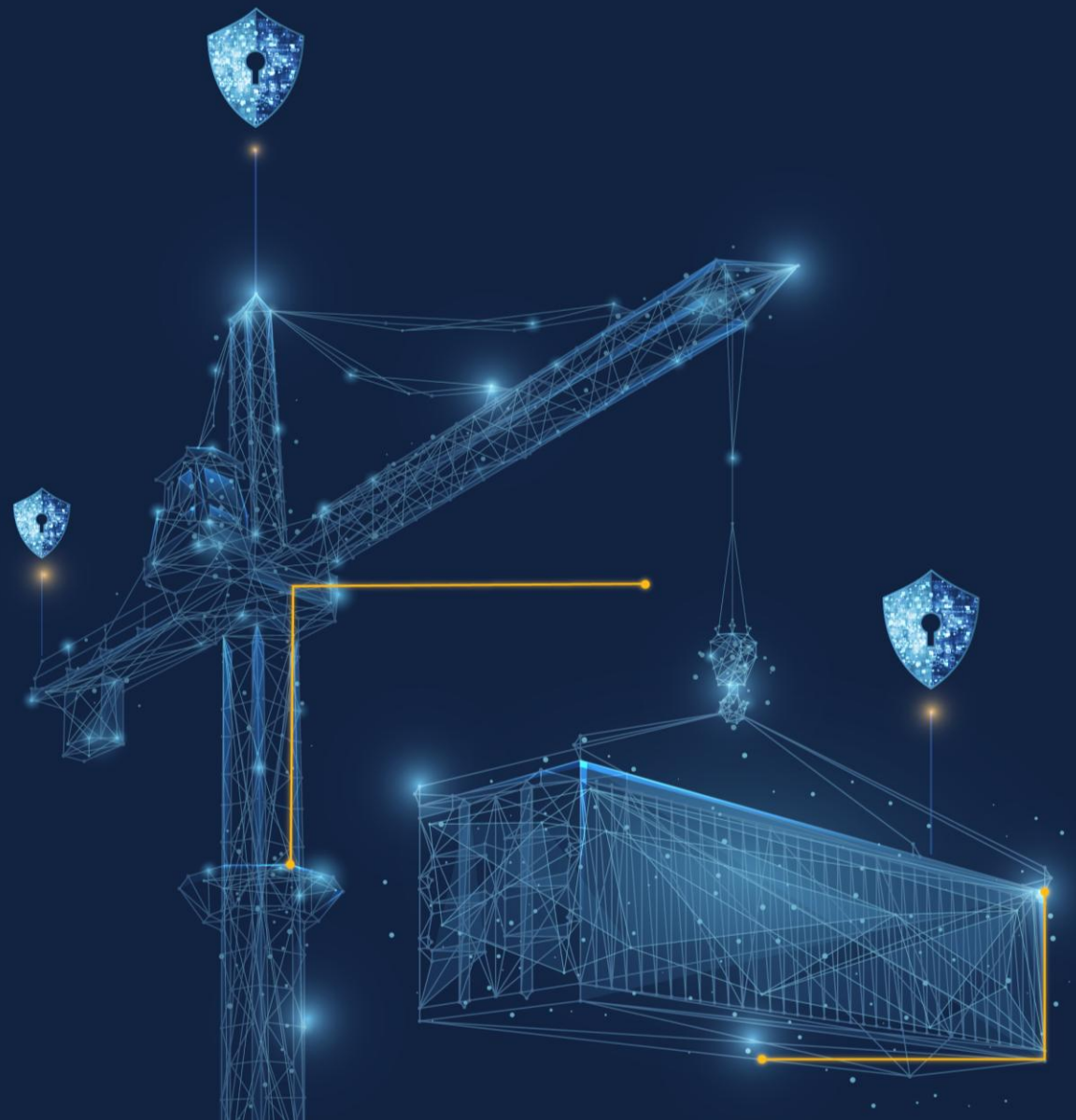
Improve Practice

- **Proactive** approach
- Regular **risk assessments**
- **Response plans**

Overcome Barriers

- **Training** and awareness
- Information **sharing**
- Aligning **incentives**

WORLD BANK GROUP



Thank You

Dominik Englert, Senior Economist, World Bank Group
denglert@worldbank.org