Cyber Risk Management In Port

Maritime Cybersecurity Dialogue 2022

Terence Yeo

AVP (Infra & Cyber Architect)

PSA Corporation Limited
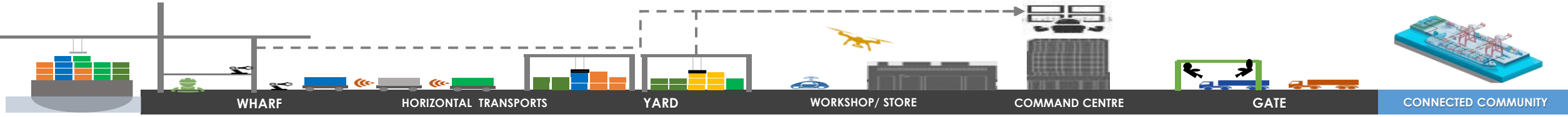
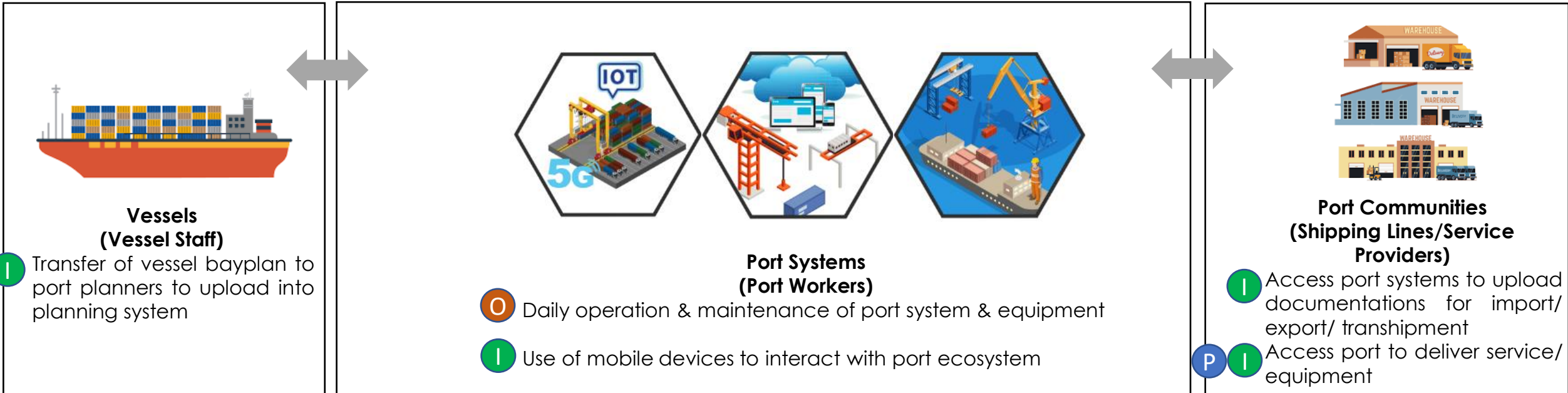# Anatomy of a Modern Port Ecosystem

With complex system interactions (Physical, IT & OT) & port users

P Physical

I IT

O OT

Automation

Hyper-connected & Orchestrated

Digitalization

WHARF HORIZONTAL TRANSPORTS YARD WORKSHOP/ STORE COMMAND CENTRE GATE CONNECTED COMMUNITY

Are technological advancement & port users posing cyber risks to port ecosystem?

Vessels (Vessel Staff)

I Transfer of vessel bayplan to port planners to upload into planning system

Port Systems (Port Workers)

O Daily operation & maintenance of port system & equipment

I Use of mobile devices to interact with port ecosystem

Port Communities (Shipping Lines/Service Providers)

I Access port systems to upload documentations for import/ export/ transhipment

P I Access port to deliver service/ equipment

Total Security Convergence: A Cyber Risk Management Approach
To strengthen competitive edge and ensure resiliency

Harmonization of Regulatory & Corporate Compliance

Strengthen Beyond Compliance

Regulatory Requirement

- CSA's Cybersecurity Code of Practice (CCOP)
- MPA's Security Standard
- MPA's International Ship and Port Facility Security (ISPS) Code
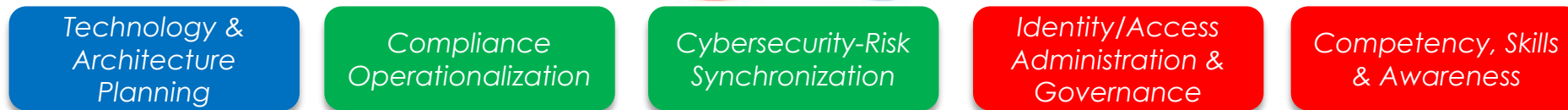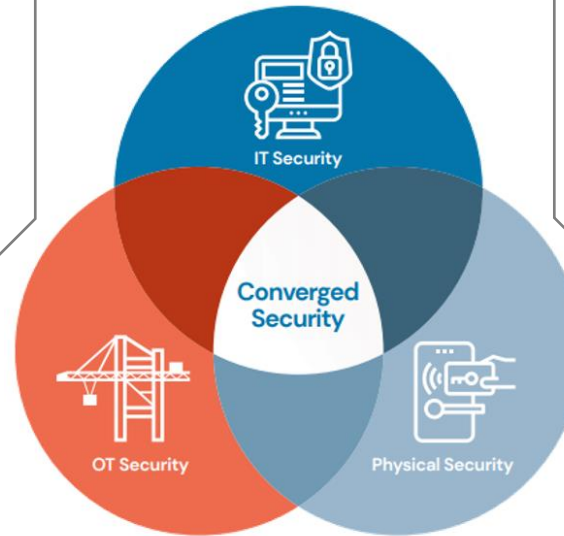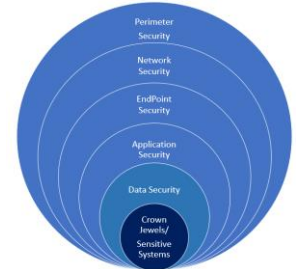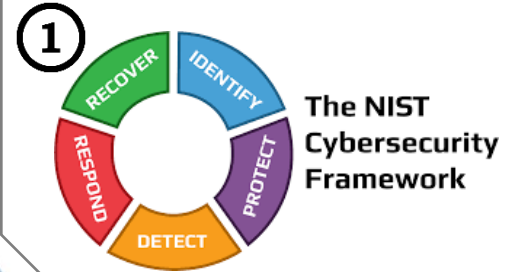- Custom's Free Trade Zone Act

Organizational Requirement

- PSA Physical/ IT/ OT Security Policy/ Standard

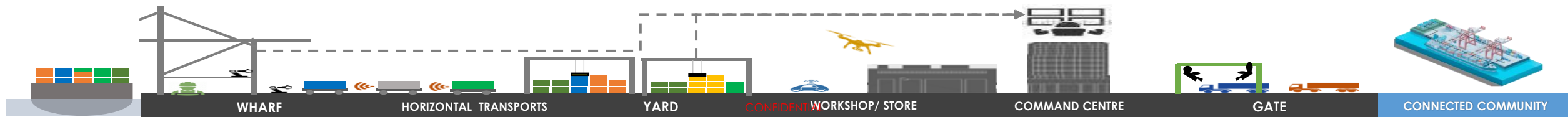**Converged Security**

IT Security
OT Security
Physical Security

Benchmark With Best Industrial Practices

- To enhance effective measures to be put in place to protect our systems against cyber attacks

① The NIST Cybersecurity Framework
RECOVER · IDENTIFY · PROTECT · DETECT · RESPOND

② MITRE ATT&CK™

③ **Defense in Depth**

Perimeter Security
Network Security
EndPoint Security
Application Security
Data Security
Crown Jewels/ Sensitive Systems

| Technology & Architecture Planning | Compliance Operationalization | Cybersecurity-Risk Synchronization | Identity/Access Administration & Governance | Competency, Skills & Awareness |

5 Key Pillars to Enable Total Security Convergence

Protect Port Systems

WHARF | HORIZONTAL TRANSPORTS | YARD | CONFIDENTIAL WORKSHOP/ STORE | COMMAND CENTRE | GATE | CONNECTED COMMUNITY

5 Key Pillars to Enable Total Security Convergence
To elevate cybersecurity posture

Technology & Architecture Planning
- Maintain **technical oversight** of IT, OT & Physical Security development roadmaps
- **Planning & co-ordination** of technology solutions for better synergy.

Compliance Operationalization
- **Coordinate & streamline implementation approach** on IT, OT & Physical security operational processes towards ensuring **sustainable compliance** to required standards
- **Lead and coordinate assessment** of **operational feasibility/implications** for compliance

Cybersecurity-Risk Synchronization
- **Establish broad based principles** to guide the alignment of IT, OT & Physical security governance towards regulatory and/or Group policies & standards
- **Align & harmonize** against various regulations & standards

Identity/Access Administration & Governance
- **Synergize & integrate** identity/access administration workflows & processes into overall organizational business processes and workflows
- **Lead formulation** of standards & guidelines on identity/access admin for IT, OT & Physical Security

Competency, Skills & Awareness
- **Identify** competency development of IT, OT & Physical security **practitioners**
- **Plan & coordinate** regular **education, awareness & outreach** activities for **internal stakeholders**

Towards A Safe & Secured Tomorrow
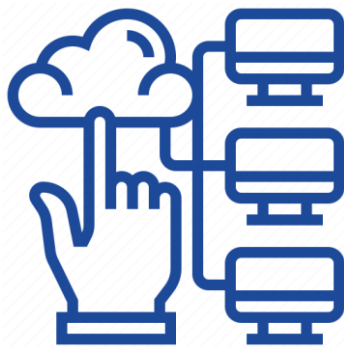*Collective Approach Partnering Key Stakeholders*

Partners / Customers

Regulators / Agencies

Solution / Service Providers

PSA Group

Thank You