Digital transformation & Cybersecurity readiness

ILIAS MANOS

AGENDA

- Digital Transformation
- Cyber Risk Management
- Cyber Resilience

Need For Digital Transformation

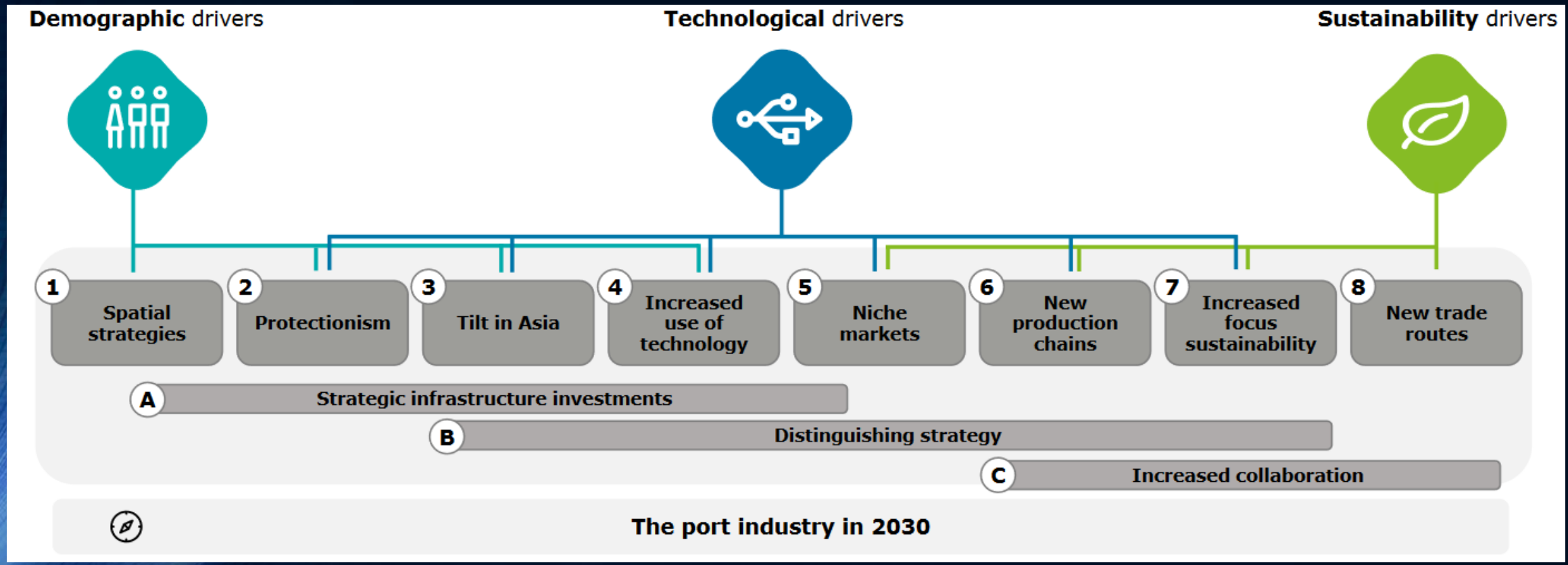
- Maritime transport is the backbone of international trade and the global economy.
- Over 80% of the volume of international trade in goods is carried by sea.
- The COVID-19 pandemic has underlined :

- the critical role that maritime ports and their associated infrastructure play in the supply chain.
- the importance to ensure business continuity and improving the resilience of critical infrastructures.

- Digital infrastructure and human capital can maximize the efficient use of the physical infrastructure.

Need For Digital Transformation : Drivers

- 80% of the 4,900 ports in the world, are not yet using digital technology and continue to rely on manual and legacy solutions, creating 'last mile' risks.
(Innovez-One)

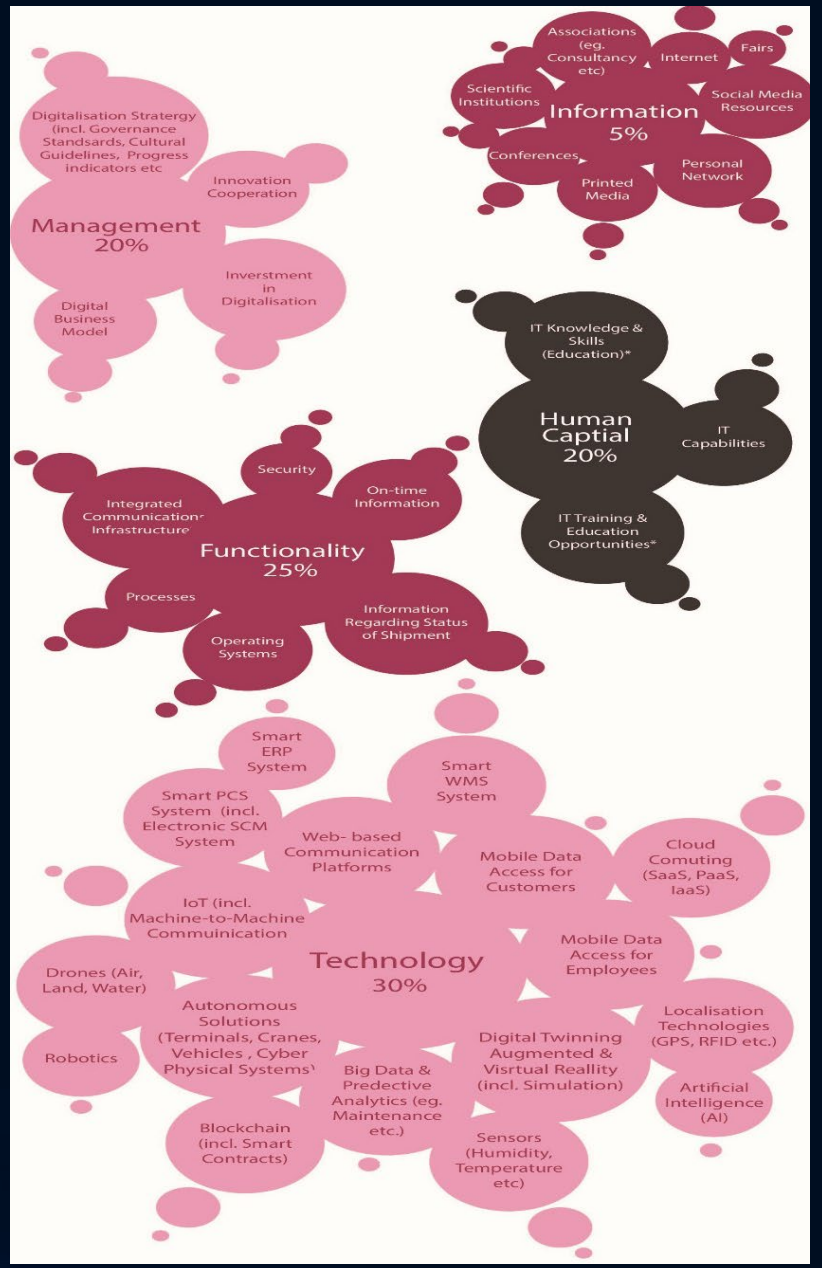


Source: Deloitte Global Port Trends 2030

Need For Digital Transformation : DRIP

- Digital Readiness Index for Ports consists of 5 dimensions and 38 related indicators:

1. Management 20%
2. Human Capital 20%
3. Functionality (IT) 25%
4. Technology 30%
5. Information 5%



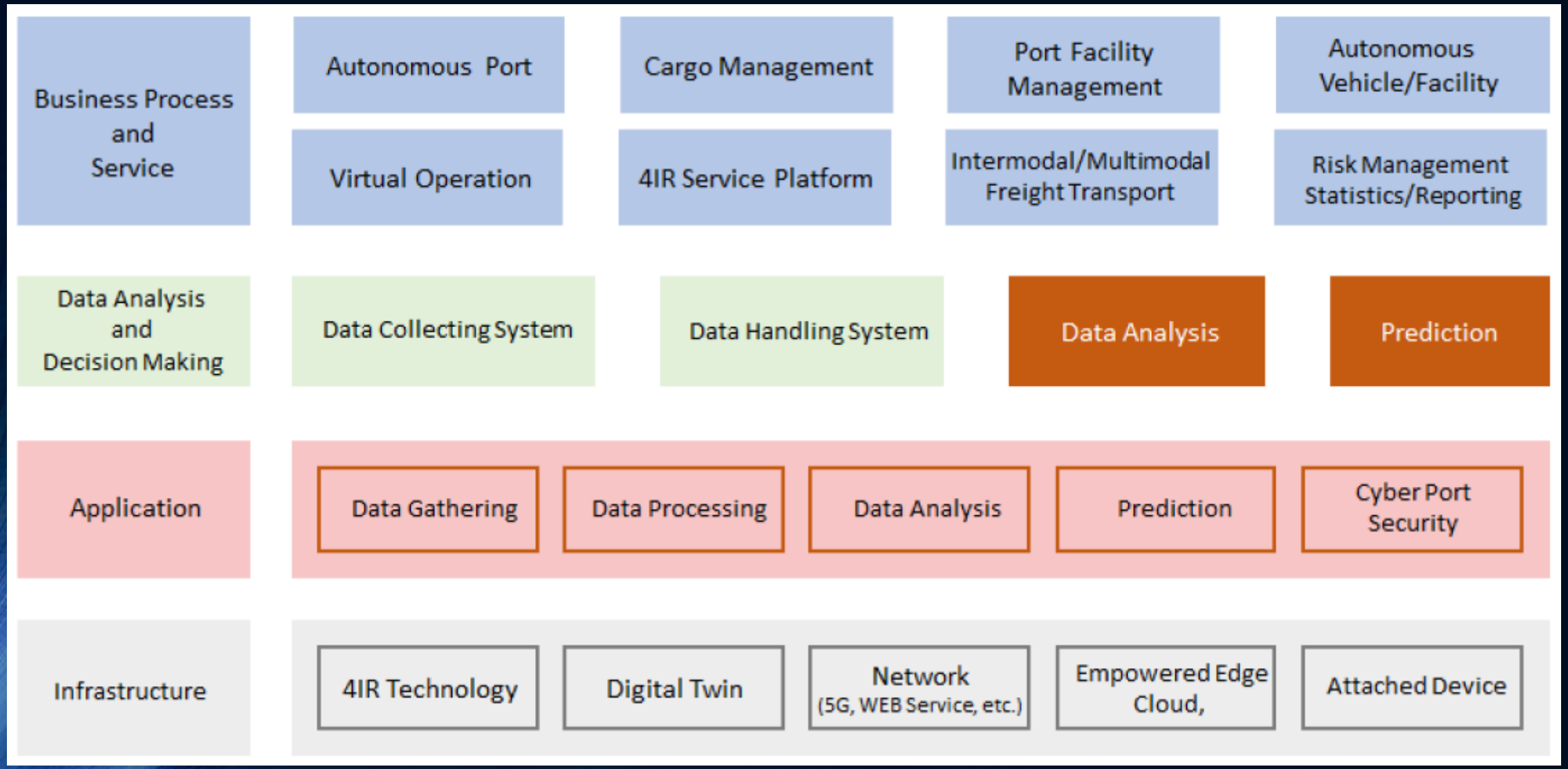
Source. Philipp et al., 2020b -& Connect2SmallPorts

Need For Digital Transformation : Smart Ports = Digital Port

A Smart Port is a port that improves its performance by using innovative technologies :

- 5G
- Wifi6
- Internet of Things (IoT)
- Big data
- Artificial Intelligence (AI)
- Advanced analytics
- Digital Twin
- Robotics process automation
- Autonomous systems
- Augmented reality (AR)
- Blockchain

Need for Digital Transformation : Framework

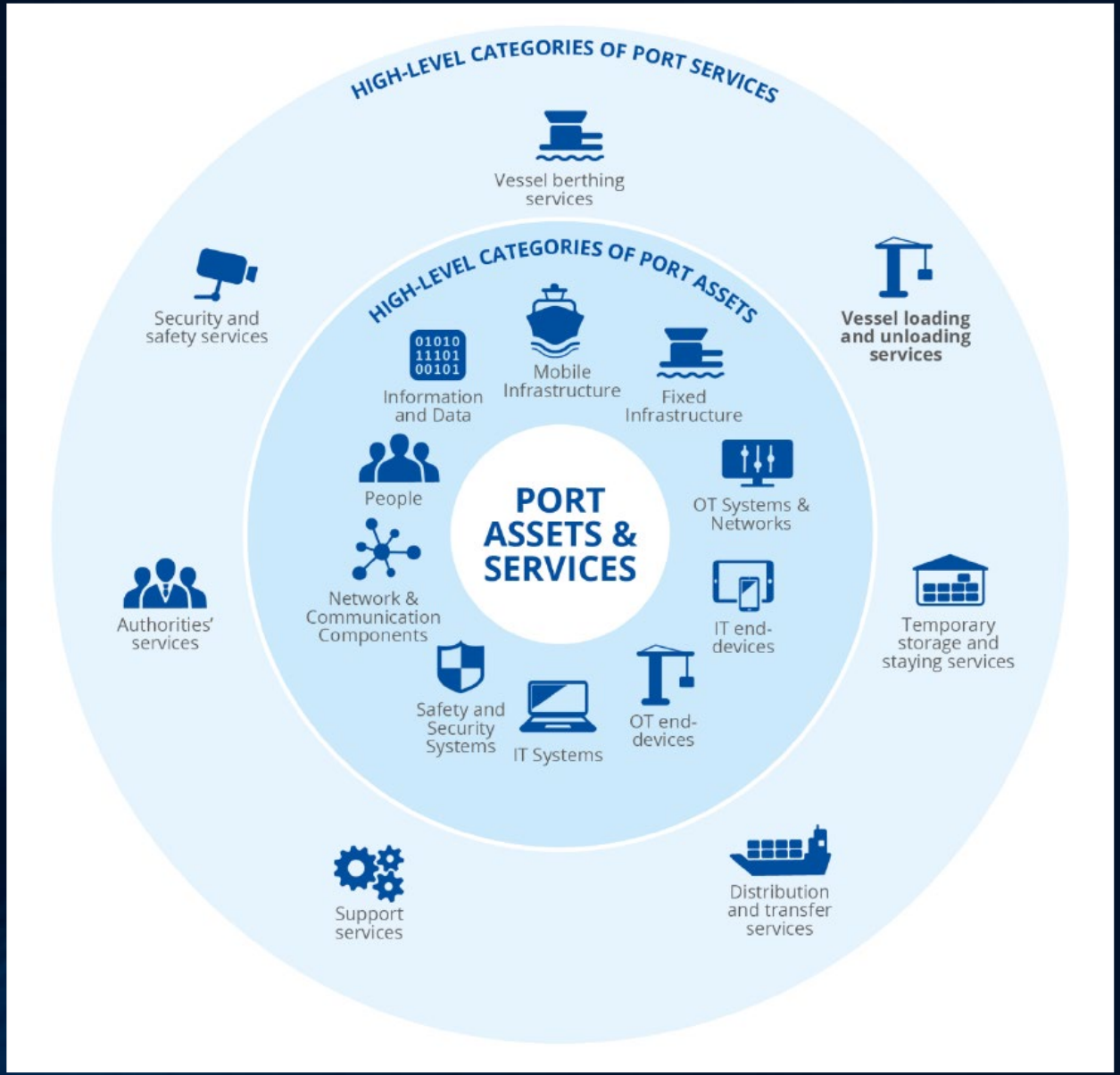


Source: ESCAP Smart Port Development

Digital Transformation
Need For
Cyber Risk Management

Phase 1: Identifying assets and services

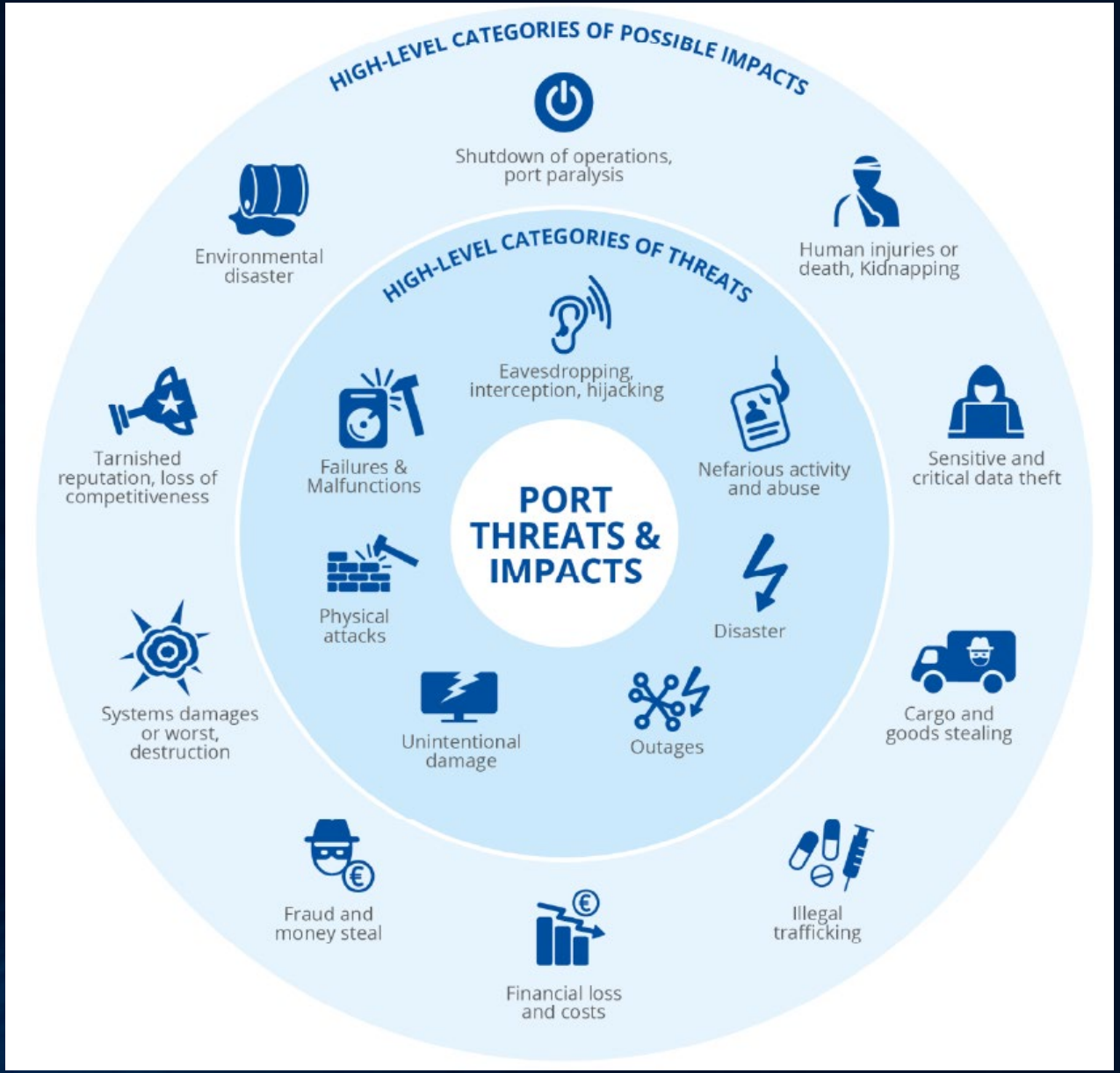
- Identify cyber-related assets and related services
- Identify internal dependencies
- Identify external dependencies with third parties
- Assess impact on the availability, integrity and confidentiality of cyber-related assets and related services



Source: ENISA - Cyber Risk Management for Ports

Phase 2: Identifying and evaluating cyber-related risks

- Identify cyber-related threats
- Identify vulnerabilities to assets and services
- Identify internal and external dependencies
- Assess the possible likelihood and impact of a cybersecurity incident
- Develop indicators (qualitative or quantitative) to evaluate identified risks



Source: ENISA - Cyber Risk Management for Ports

Phase 3: Identifying security measures

- Identify security measures to mitigate identified risks
- Assess the effectiveness and impact of the security measures
- Assess resource requirements for the implementation of security measures
- Define a process for prioritizing security measures

- ✓ Security policy and organization
- ✓ Risk and Threats
- ✓ Security and privacy by design
- ✓ Asset inventory and management
- ✓ Business continuity and crisis management
- ✓ Endpoints protection and lifecycle management
- ✓ Vulnerabilities management
- ✓ Human resource security
- ✓ Supply chain management
- ✓ Detection and incident response
- ✓ Control and auditing
- ✓ IT and OT physical protection
- ✓ Network security
- ✓ Access control
- ✓ Administration and Configuration Management
- ✓ Threat management
- ✓ Cloud security
- ✓ Data protection
- ✓ Update management
- ✓ Detection and monitoring
- ✓ Industrial control systems security
- ✓ Backup and restore

Source: ENISA - Cyber Risk Management for Ports

Phase 4: Assessing cybersecurity maturity

- Assess cybersecurity capabilities over three maturity levels and dual progression:

➢ Capability progression

measures the degree to which the organisation has implemented cybersecurity capabilities (people, processes, tools, and funding).

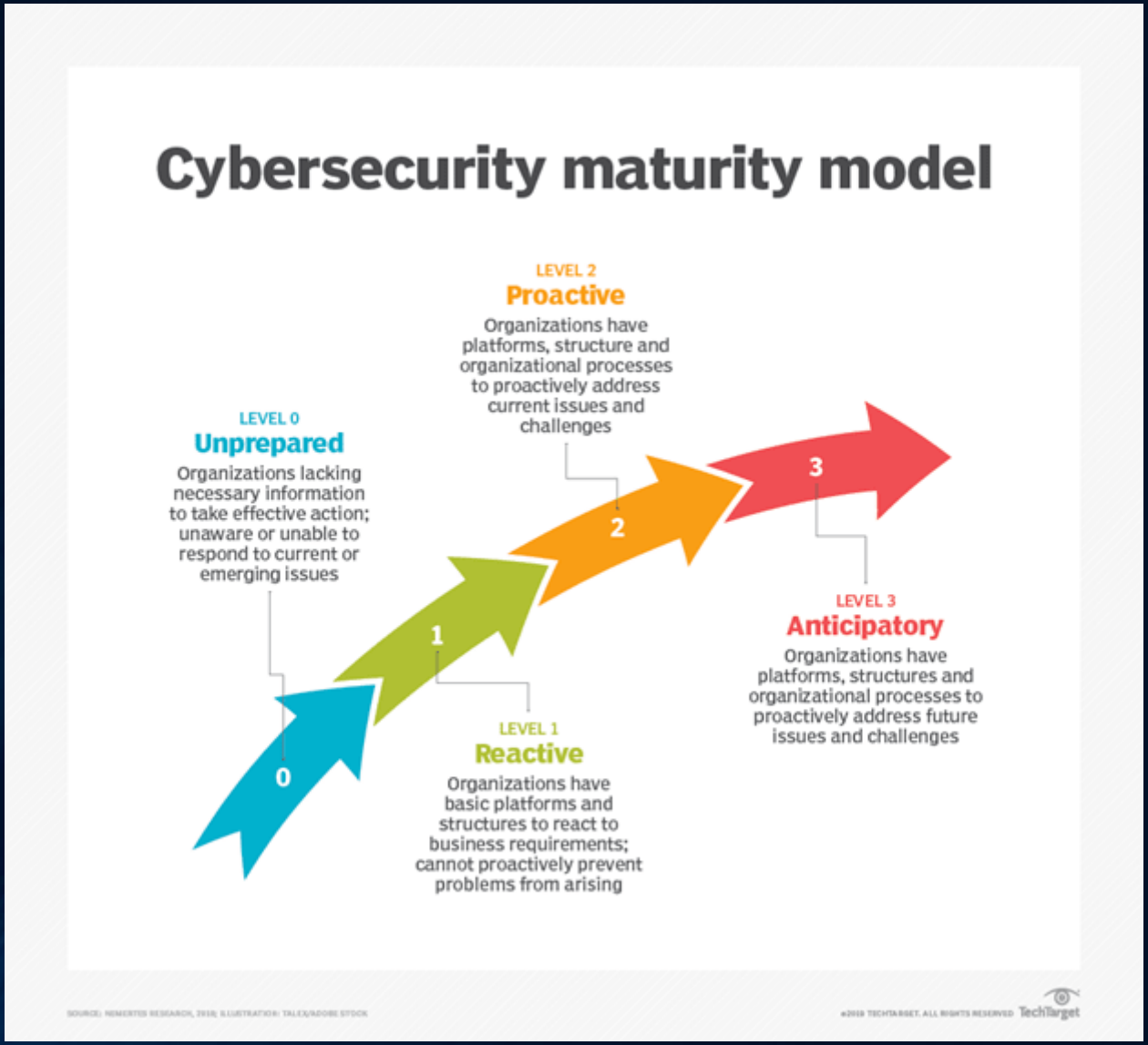
➢ Institutionalisation

measures how deeply entrenched specific activities, controls, processes, and procedures are within and across the organisation.

Maturity Level	Description
1 (Basic)	This level corresponds to the minimum-security measures that are implemented to achieve a security objective. The organisation performs baseline activities and/or capabilities, even in an ad hoc manner.
2 (Intermediate)	This level corresponds to more sustained capabilities that align with identified standards and best practices. The organisation implements, manages, monitors, and measures capabilities against defined objectives and operational applicability. Documentation (i.e. plans and policies) guides the application and utilisation of resources for specific and/or coordinated activities.
3 (Optimal)	This level corresponds to activities and/or capabilities that are planned, tested, policy-informed, and repeatable; subject to regular oversight and reviews to confirm effectiveness; and improve the implementation of security measures, taking into account disciplined changes, tests, and exercises. The organisation regularly measures capabilities to support continuous improvement efforts to attain and sustain defined performance objectives.

Phase 4: Assessing cybersecurity maturity

- Level 0: Unprepared. This organization lacks the people, processes and technology to deal with cybersecurity threats.
- Level 1: Reactive. This organization has the people, processes and technology in place to handle attacks after they've occurred.
- Level 2: Proactive. This organization has the people, processes and technology in place to protect against foreseeable threats from known sources.
- Level 3: Anticipatory. This organization has the people, processes and technology to protect against threats that could emerge based on changes in the business and technology environment.

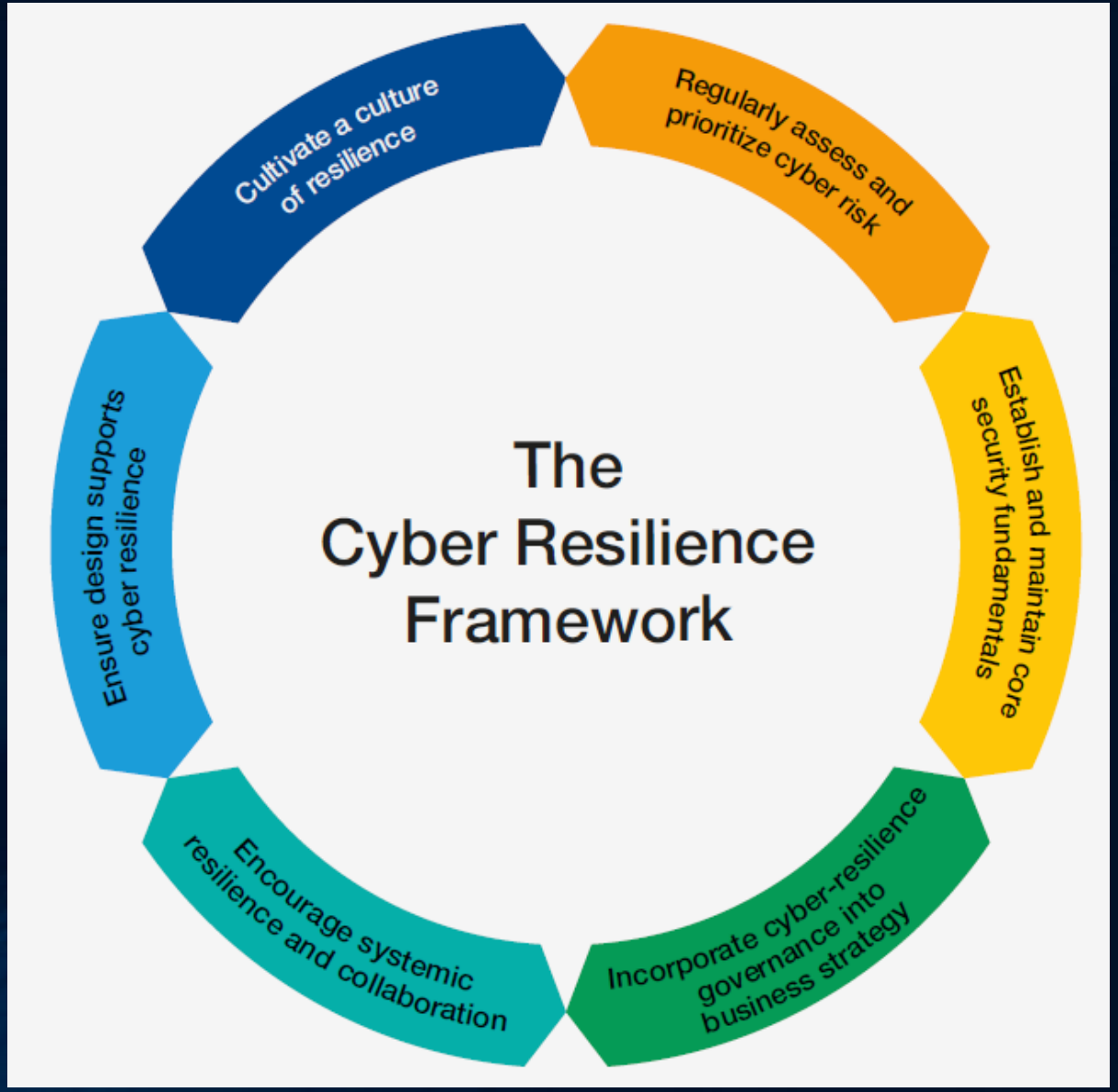


Nemertes Research NIST Cybersecurity Framework Simplified

Cyber security is never enough: Businesses need cyber resilience

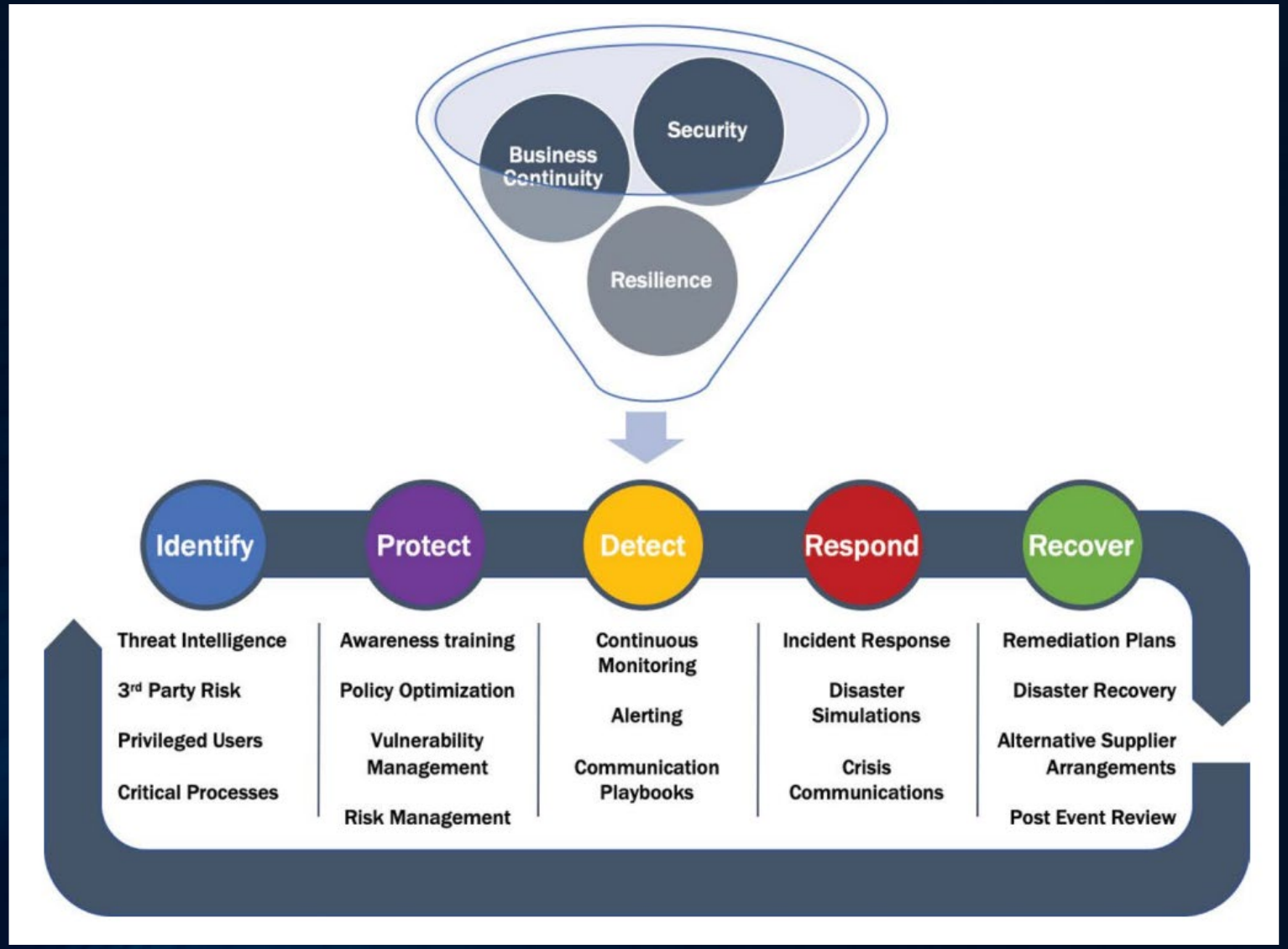
Cyber Resilience Framework

- Regularly assess and prioritize cyber risk
- Establish and maintain core security fundamentals
- Incorporate cyber-resilience governance into business strategy
- Encourage systemic resilience and collaboration
- Ensure design supports cyber resilience (resilience by design)
- Cultivate a culture of resilience



Source: World Economic Forum and Accenture

Components of Cyber Resiliency



Thank you