Bureau Veritas

Cybersecurity Ecosystem

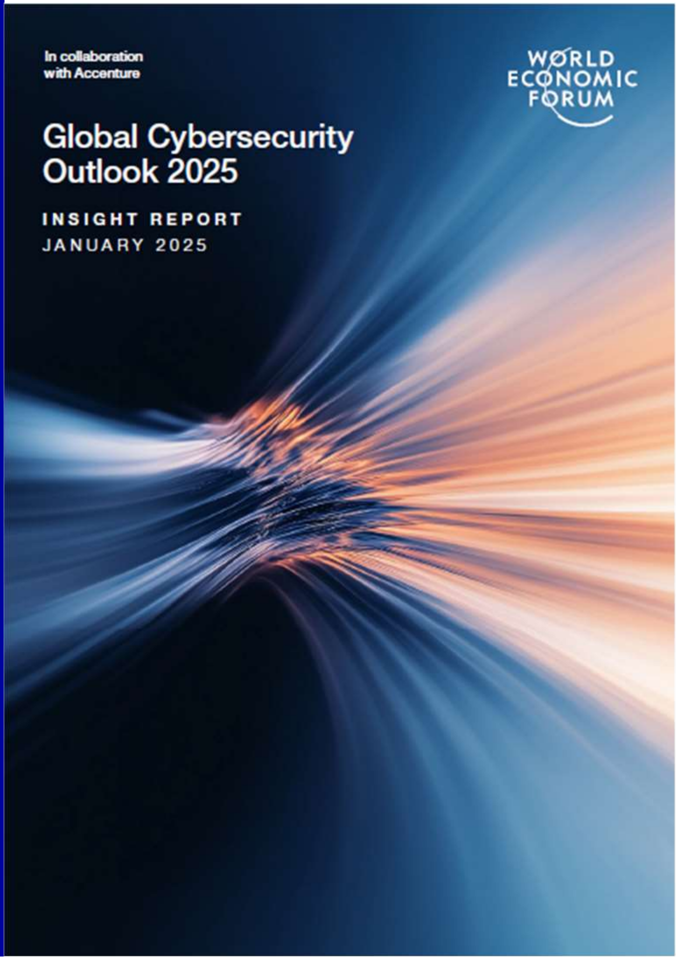
Hila Ahmadi

October 2025

MARITIMEBRIEFING

more to sea.

INTRODUCTION


In collaboration with Accenture

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2025

INSIGHT REPORT

JANUARY 2025

“In a complex cyberspace characterized by geopolitical uncertainties, widening cyber inequity and sophisticated cyber threats, leaders must adopt a security-first mindset.

2025’s report shines a light on the increasing complexity of the cyber landscape, which has profound and far-reaching implications for organizations and nations.

This complexity is driven by a series of compounding factors:

- Escalating geopolitical tensions are contributing to a more uncertain environment.
- Increased **integration** of and dependence on more complex supply chains is leading to a more opaque and unpredictable risk landscape.
- The rapid adoption of emerging technologies is contributing to new vulnerabilities as cybercriminals harness them effectively to achieve greater sophistication and scale.
- Simultaneously, the proliferation of **regulatory requirements** around the world is adding a significant compliance burden for organizations.

Source: « WEF Global Cybersecurity Outlook 2025»

https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Maritime Market Threats & Challenges

MARITIME DIGITAL EVOLUTION

Globalised Shipping Management

Performance monitoring

- Vessels operations are digitalized and managed from the shore

Growing connectivity

On-board networks interconnections

- Connected propulsion or navigation systems
- SatCom provide growing access to any part of the vessels

Smart Shipping

Predictive Maintenance

- Sensors & IoT
- Efficiency
- Remote Maintenance
- Real-Time monitoring
- Data Science

Digital Twin

Accurate Prediction

- Correlation with external sources
- Machine Learning
- Minimized risk of human error
- Enhanced port & terminal operations
- End-to-end supply chain optimization

Unmanned Vessels

Fully remotely controlled

- All systems remotely operated
- No more manual ship handing over

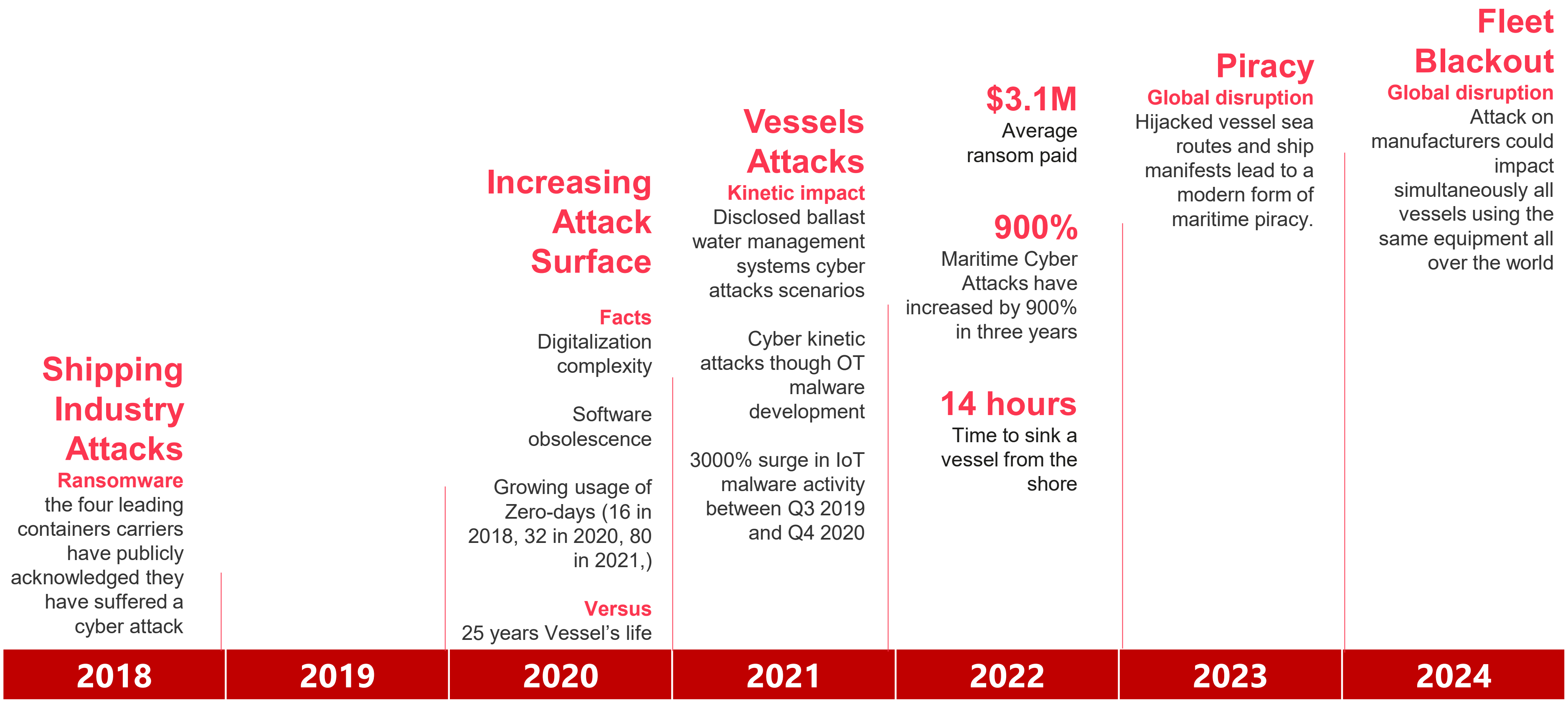
Autonomous Vessels

Artificial Intelligence

- Operations and safety rely at 100% on onboard systems

<2018	2019	2020	2021	2022	2023	2024+

MARITIME THREATS EVOLUTION



Shipping Industry Attacks

Ransomware

the four leading containers carriers have publicly acknowledged they have suffered a cyber attack

Increasing Attack Surface

Facts

Digitalization complexity

Software obsolescence

Growing usage of Zero-days (16 in 2018, 32 in 2020, 80 in 2021,)

Versus

25 years Vessel's life

Vessels Attacks

Kinetic impact

Disclosed ballast water management systems cyber attacks scenarios

Cyber kinetic attacks though OT malware development

3000% surge in IoT malware activity between Q3 2019 and Q4 2020

$3.1M

Average ransom paid

900%

Maritime Cyber Attacks have increased by 900% in three years

14 hours

Time to sink a vessel from the shore

Piracy

Global disruption

Hijacked vessel sea routes and ship manifests lead to a modern form of maritime piracy.

Fleet Blackout

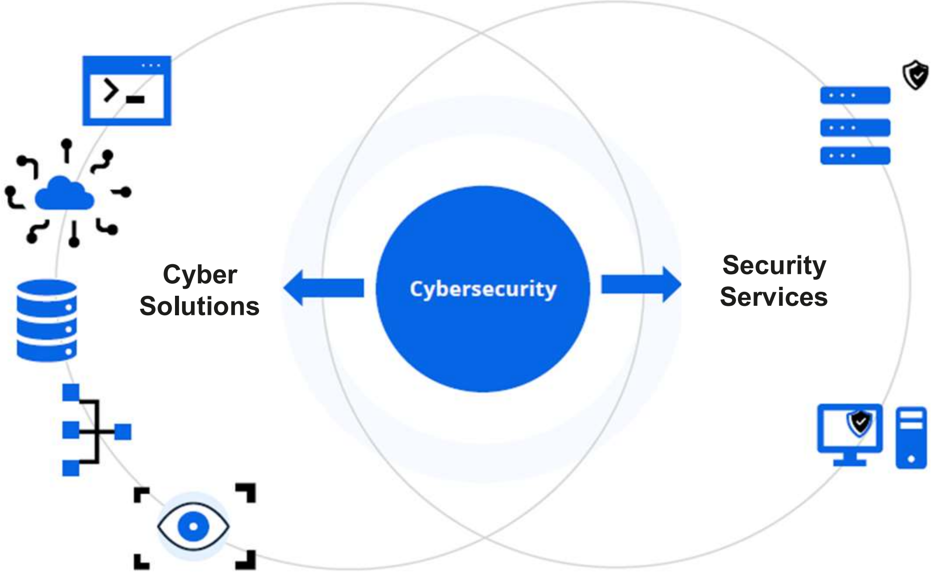
Global disruption

Attack on manufacturers could impact simultaneously all vessels using the same equipment all over the world

THE MARITIME MARKET

KEY DRIVERS

- ➢ Increasing adoption of IoT, cloud computing, and other digital technologies in maritime operations
- ➢ Rising threats of cyber attacks targeting ships, ports, and maritime supply chains
- ➢ Stringent regulations and guidelines around maritime cybersecurity (e.g. IMO, IACS)
- ➢ Need to protect critical maritime infrastructure and ensure business continuity



MAJOR MARKET SEGMENTS:

- ➢ **Solutions** (firewalls, antivirus, encryption, etc.)
- ➢ **Services** (consulting, integration, managed services, etc.)
- ➢ **End-users** (commercial shipping, naval defense, ports and terminals, etc.)

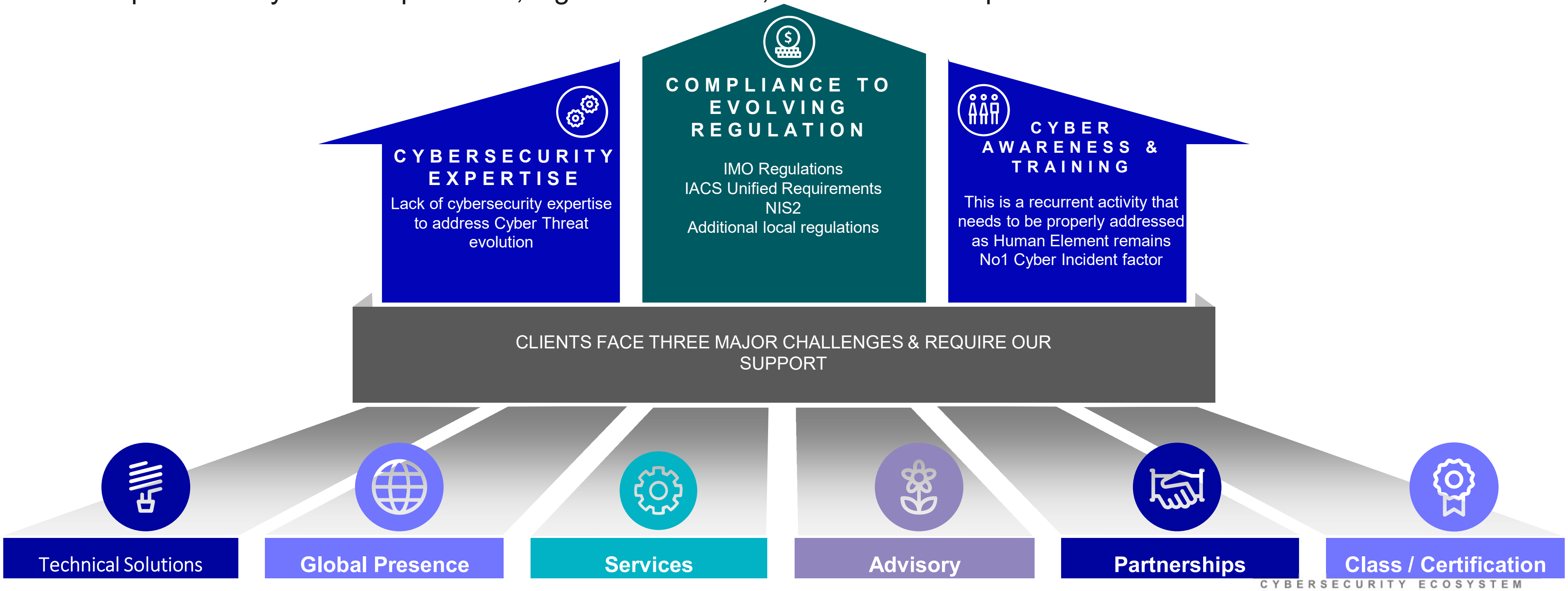
REGIONAL ANALYSIS:

- ➢ **North America** and **Europe** are the largest and most mature markets currently.
- ➢ **Asia-Pacific** is expected to be the fastest growing region due to expansion of maritime trade and investments in port infrastructure.

**Source: Research and Markets Report:*
"Global Maritime Cybersecurity Market Report 2022-2027"
Published: January 2022

MARITIME CYBERSECURITY & CHALLENGES

- Fosters trust and confidence among stakeholders, such as shipping companies, port authorities, and clients
- Establishing this trust is vital for maintaining business partnerships, attracting investments, and fostering industry growth.
- Adhering to stringent cybersecurity protocols is essential for meeting international regulations and industry standards, such as those mandated by the International Maritime Organization (IMO) and the International Ship and Port Facility Security (ISPS) Code.
- Non-compliance may result in penalties, legal ramifications, and tarnished reputations.



CYBERSECURITY EXPERTISE

Lack of cybersecurity expertise to address Cyber Threat evolution

COMPLIANCE TO EVOLVING REGULATION

IMO Regulations
IACS Unified Requirements
NIS2
Additional local regulations

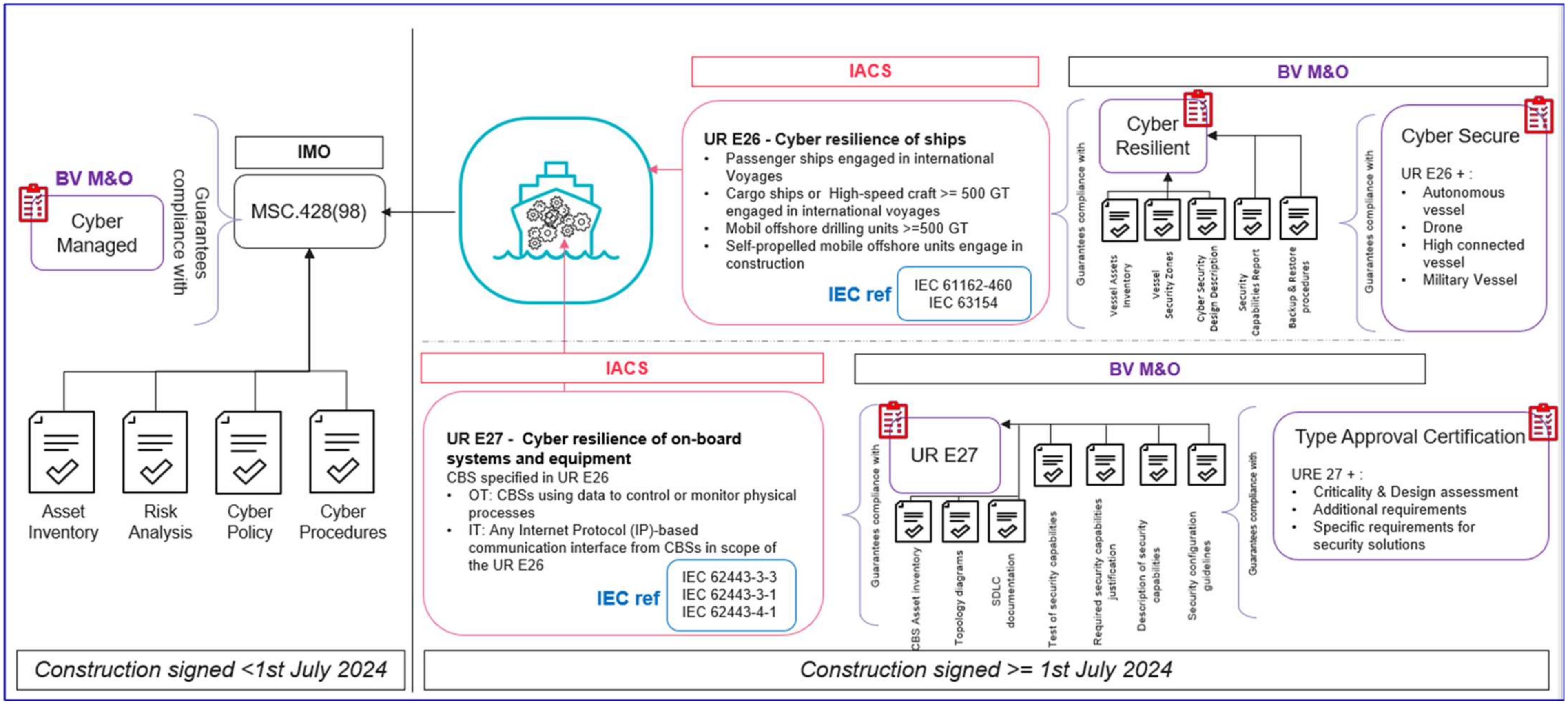
CYBER AWARENESS & TRAINING

This is a recurrent activity that needs to be properly addressed as Human Element remains No1 Cyber Incident factor

CLIENTS FACE THREE MAJOR CHALLENGES & REQUIRE OUR SUPPORT

Regulatory Landscape

CYBER CLASS AND CERTIFICATION



UR E26 - Cyber resilience of ships

- Passenger ships engaged in international Voyages
- Cargo ships or High-speed craft >= 500 GT engaged in international voyages
- Mobil offshore drilling units >=500 GT
- Self-propelled mobile offshore units engage in construction

IEC ref: IEC 61162-460, IEC 63154

UR E27 - Cyber resilience of on-board systems and equipment

CBS specified in UR E26

- OT: CBSs using data to control or monitor physical processes
- IT: Any Internet Protocol (IP)-based communication interface from CBSs in scope of the UR E26

IEC ref: IEC 62443-3-3, IEC 62443-3-1, IEC 62443-4-1

Cyber Secure

UR E26 + :

- Autonomous vessel
- Drone
- High connected vessel
- Military Vessel

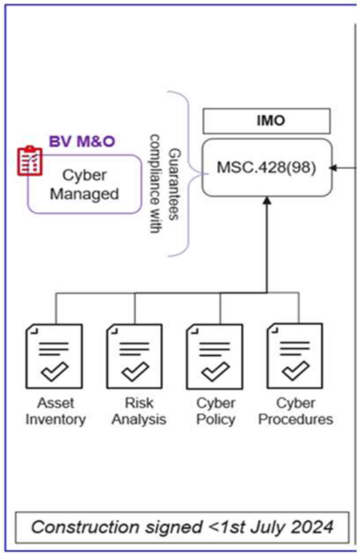
Type Approval Certification

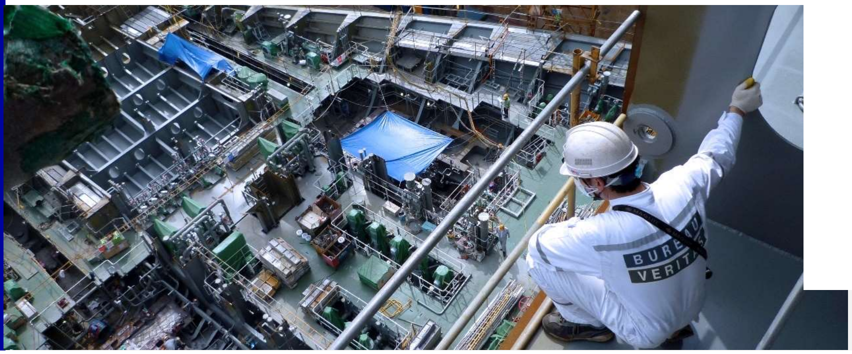
URE 27 + :

- Criticality & Design assessment
- Additional requirements
- Specific requirements for security solutions

BV M&O
Cyber Managed
Guarantees compliance with
IMO
MSC.428(98)
Asset Inventory
Risk Analysis
Cyber Policy
Cyber Procedures
Construction signed <1st July 2024
IACS
IEC ref
BV M&O
Cyber Resilient
Guarantees compliance with
Vessel Assets Inventory
Vessel Security Zones
Cyber Security Design Description
Security Capabilities Report
Backup & Restore procedures
Guarantees compliance with
IACS
BV M&O
UR E27
Guarantees compliance with
CBS Asset inventory
Topology diagrams
SDLC documentation
Test of security capabilities
Required security capabilities justification
Description of security capabilities
Security configuration guidelines
Guarantees compliance with
Construction signed >= 1st July 2024

CYBER MANAGED





STRICT IMO COMPLIANCE

CYBER MANAGED provides a direct IMO MSC 428(98) Compliance and at the same time is considered an enabler for Cyber in the Maritime Industry

« ADMINISTRATIONS ARE ENCOURAGED TO ENSURE THAT CYBER RISKS ARE APPROPRIATELY ADDRESSED IN SAFETY MANAGEMENT SYSTEMS »

More and more **FLAG STATE INSPECTORS** are starting to seriously take into consideration cyber security management on board.

PORT STATE CONTROLS are likely to follow this trend.

RIGHTSHIP now includes cyber security in their vetting process.

« AN APPROVED SAFETY MANAGEMENT SYSTEM SHOULD TAKE INTO ACCOUNT CYBER RISK MANAGEMENT »

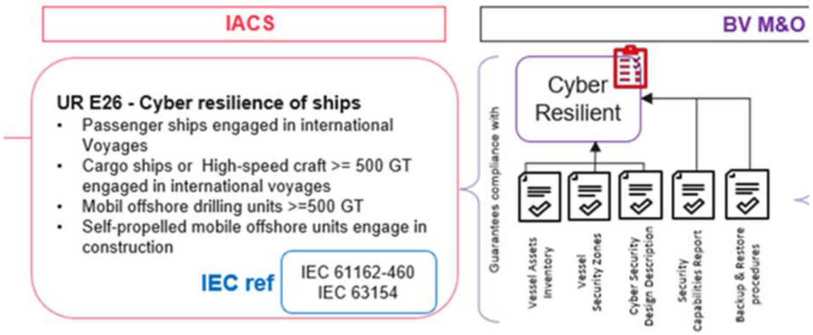
ASSETS INVENTORY (systems, equipment, networks, interconnections, incl. remote access and ship connection with shore)

RISK ANALYSIS : threats, effects, impacts, criticality
Mitigation measures already implemented or to be applied

Shipowner's CYBER SECURITY POLICY **SMS**
Roles, rules, responsabilites, crew training, crisis management

Onboard **PROCEDURES** to implement Cyber Security Policy
Monitoring, maintenance, incident response **SMS**

CYBER RESILIENT



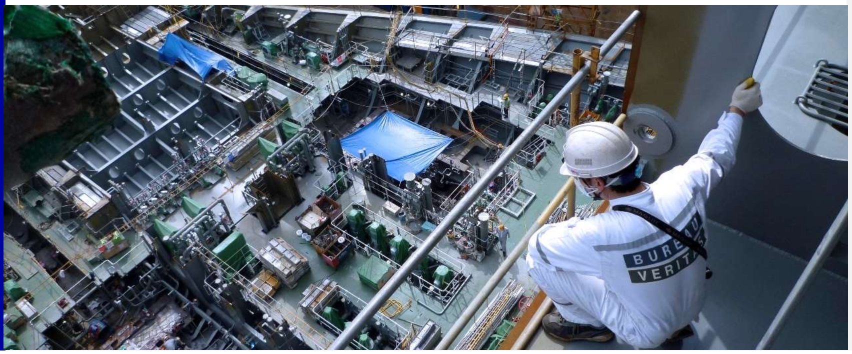
IACS

UR E26 - Cyber resilience of ships
- Passenger ships engaged in international Voyages
- Cargo ships or High-speed craft >= 500 GT engaged in international voyages
- Mobil offshore drilling units >=500 GT
- Self-propelled mobile offshore units engage in construction

IEC ref

IEC 61162-460
IEC 63154

BV M&O
Guarantees compliance with
Cyber Resilient
Vessel Assets Inventory
Vessel Security Zones
Cyber Security Design Description
Security Capabilities Report
Backup & Restore procedures



STRICT UR E26 COMPLIANCE

CYBER RESILIENT Chapter in NR 659 contains word for word IACS UR E26.

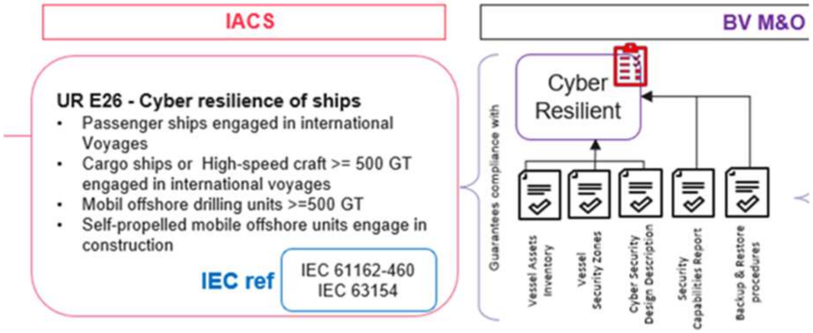
FIVE REQUESTED DELIVERABLES

Vessel digital assets inventory, zones and conduct diagram, cybersecurity design description, cyber risk analysis (only to exclude systems or equipment from scope) and cyber resilience test procedures.

NOT A ONE SHOT!!!

Yards will be the first to prepare the required documentation but, as CYBER RESILIENT will have to be maintained. Shipowners will have to keep this documentation updated during whole lifecycle of their vessels. That’s a huge challenge that will probably be sub-contracted…

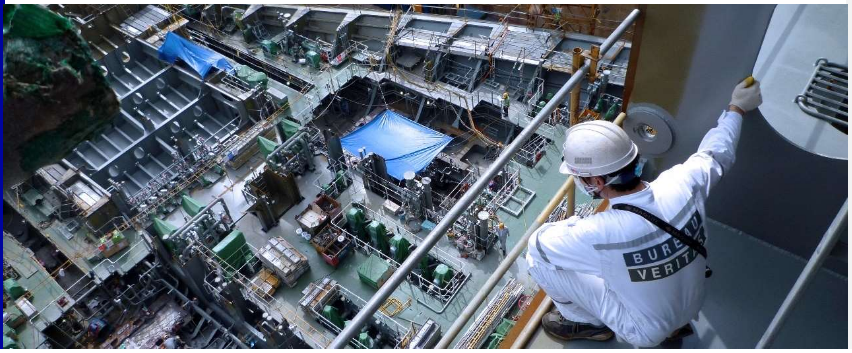
CYBER RESILIENT


IACS
BV M&O
Cyber Resilient
Guarantees compliance with
Vessel Assets Inventory
Vessel Security Zones
Cyber Security Design Description
Security Capabilities Report
Backup & Restore procedures
IEC ref

UR E26 - Cyber resilience of ships

- Passenger ships engaged in international Voyages
- Cargo ships or High-speed craft >= 500 GT engaged in international voyages
- Mobil offshore drilling units >=500 GT
- Self-propelled mobile offshore units engage in construction

IEC 61162-460
IEC 63154



PIPELINE

As per 2025, April 8th, **more than 130 vessels** have been assigned the CYBER RESILIENT feature or notation.

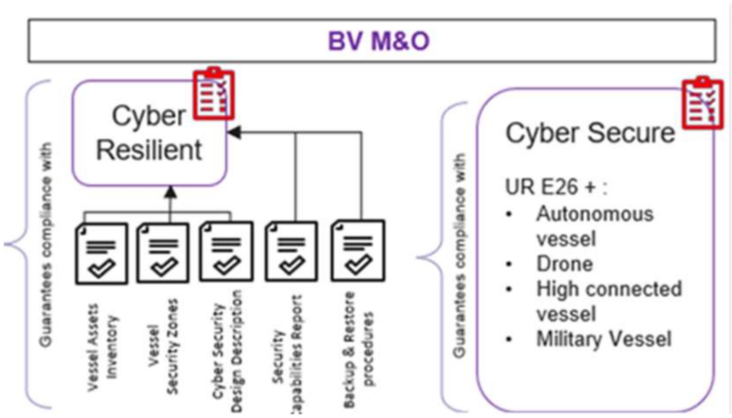
BEST PRACTICE

A dedicated cybersecurity meeting must be scheduled at very early project stage between Yard, Owner and main vendors. Responsibilities (and need for support?) must be defined.

SYSTEMS INTEGRATOR

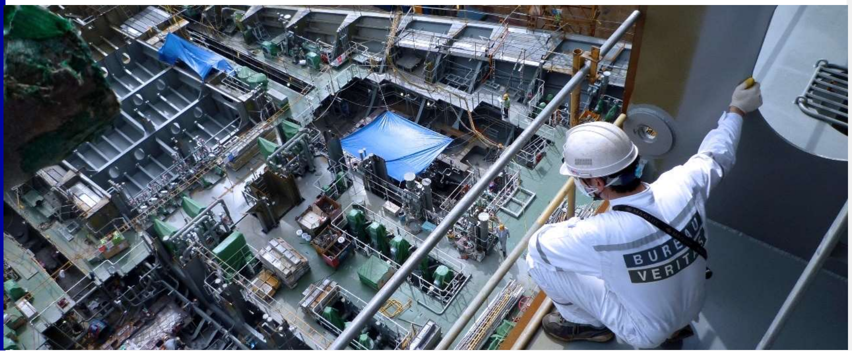
A new role created by UR E26. He's the link between Yard, Owner and main vendors. He will collect information from all stakeholders to draft the required deliverables. He must be identified and his responsibilities must be defined by agreement between Yard and Owner.

CYBER SECURE


BV M&O
Guarantees compliance with
Cyber Resilient
Vessel Assets Inventory
Vessel Security Zones
Cyber Security Design Description
Security Capabilities Report
Backup & Restore procedures
Guarantees compliance with
Cyber Secure

UR E26 + :

- Autonomous vessel
- Drone
- High connected vessel
- Military Vessel



ENHANCED UR E26 COMPLIANCE

CYBER SECURE requirements will include CYBER RESILIENT requirements, hence will guarantee compliance with UR E26 & UR E27. Extra requirements will rely on the DETECT/PROTECT pillars of the NIST framework.

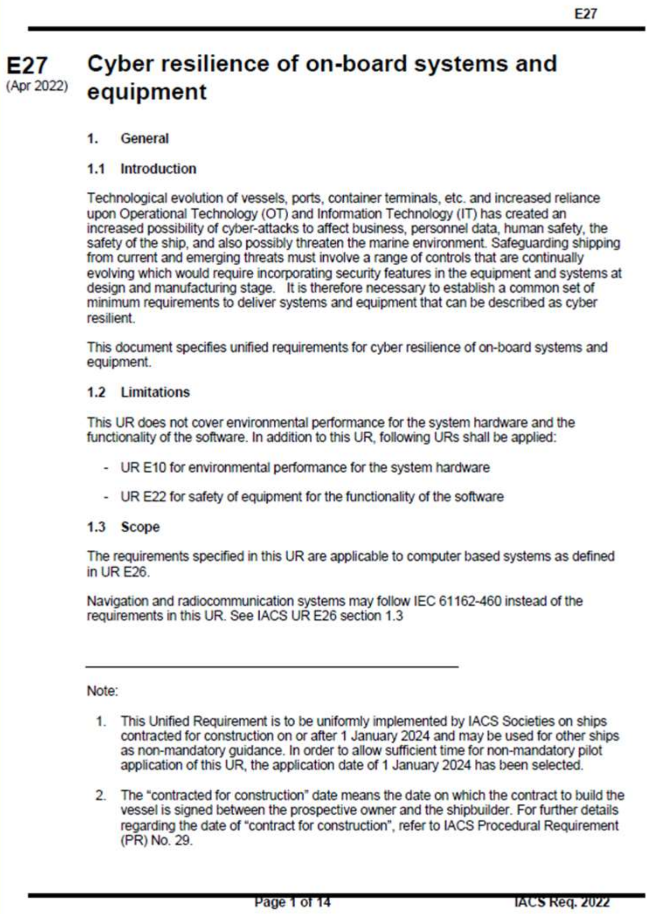
A MODULAR NOTATION

CYBER SECURE will contain a base of additional requirements + dedicated specific modules (MASS, NAVY…)

EXPECTED AVAILABILITY : JAN 2026

Current CYBER SECURE is too ambitious and not adapted to what the suppliers can provide today. Only a part of it is implementable. The challenge for the new notation is to be more demanding than UR E26 while taking into consideration, not only what the maritime suppliers are able to provide but also the specific needs to certain type of vessels. For military vessels, a Joint Development Project has been initiated with Naval Group.

REGULATIONS – UR E27



E27

E27 (Apr 2022)

Cyber resilience of on-board systems and equipment

1. General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

1.3 Scope

The requirements specified in this UR are applicable to computer based systems as defined in UR E26.

Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in this UR. See IACS UR E26 section 1.3

Note:

1. This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance. In order to allow sufficient time for non-mandatory pilot application of this UR, the application date of 1 January 2024 has been selected.
2. The "contracted for construction" date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of "contract for construction", refer to IACS Procedural Requirement (PR) No. 29.

Page 1 of 14 IACS Req. 2022

UR E27 «*Cyber Resilience of Onboard Systems and Equipment*» aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment and provides additional requirements relating to interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard vessels.

As UR E27 relies mostly on IEC62443-3-3 (and a little bit on IEC 62443-4-1), a vendor already IEC 62443 certified will have no problem getting the UR E27 certification. As required documentation will already be on shelves, UR E27 certification in that case will almost be an administrative work.

Our Services Portfolio

CYBER SERVICES - BV CYBERSECURITY

Human Element

- □ Social Engineering
- □ E-learning
- □ Training Courses
  - □ Yard
  - □ Owner
- □ Cyber Drills
- □ Incident Response
- □ Tabletop Crisis Management

Regulatory Compliance

- □ Security Maturity Assessment
- □ Security Management Implementation
- □ Advisory Services
- □ IT / OT Assessment

Technology

IT ↔ OT

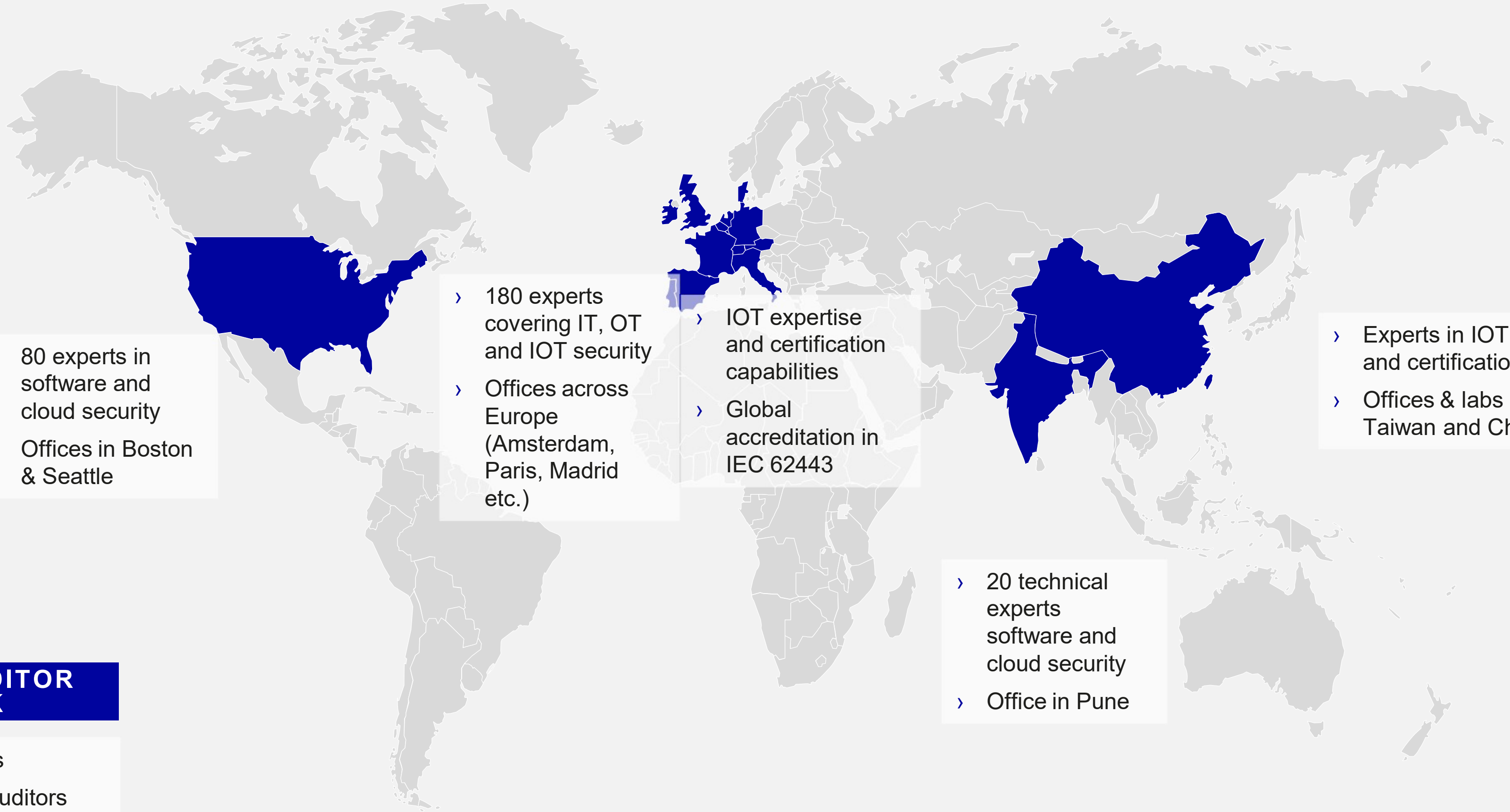
IT

- □ IT Pen-testing
- □ Design Review
- □ Threat Modeling
- □ External Attack Surface Assessment

OT

- □ Site Assessment
- □ NIS2 Services
- □ Threat Modeling
- □ OT Pen-testing

BV CYBERSECURITY GLOBAL PRESENCE



- 80 experts in software and cloud security
- Offices in Boston & Seattle

- 180 experts covering IT, OT and IOT security
- Offices across Europe (Amsterdam, Paris, Madrid etc.)

- IOT expertise and certification capabilities
- Global accreditation in IEC 62443

- Experts in IOT testing and certification
- Offices & labs in Taiwan and China

- 20 technical experts software and cloud security
- Office in Pune

+ GLOBAL AUDITOR NETWORK

- EU – 3,500+ auditors
- Americas – 1,100+ auditors
- EMEA – 900+ auditors
- APAC – 1,800+ auditors

Vielen Dank für Ihre Aufmerksamkeit!

www.maritime-briefing.de

Hier geht´s zu den Vorträgen und Kontaktdaten unserer Gastgeber!

MARITIMEBRIEFING

more to sea.

BUREAU VERITAS 1828

BUREAU VERITAS

BELFS

NW Assekuranz
Global Insurance Broking

CLA dhpg