SAFETY, RISK AND COMPLIANCE MANAGEMENT

A PRIMER ON IMO CYBER RISK MANAGEMENT GUIDELINES

What to Know and How to Comply

ABS Group | THE AMERICAN CLUB 1917

Table of Contents

Organizations are encouraged to address cyber risk management in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Maritime cybersecurity has been a topic of confusion and debate for the past 20 years. Within the last 5 years, governments, flag administrations and ship owners and operators have stepped in to provide recommendations and guidance as to how the marine industry can effectively manage evolving cyber threats as a major safety concern and operational risk.

> Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. – IMO

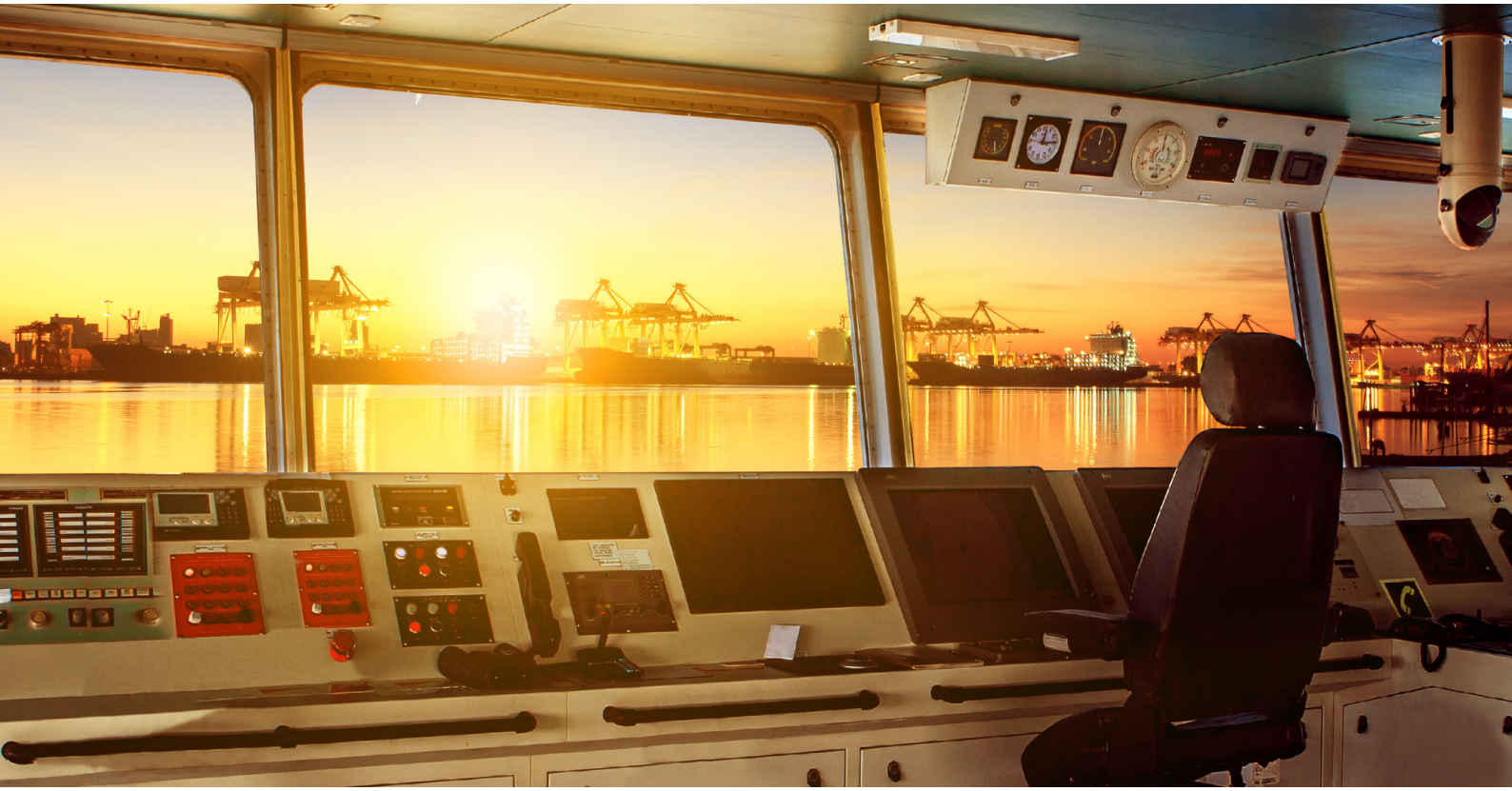
The International Maritime Organization (IMO) promotes the safety of life at sea and the environment. In 2017, IMO released the circular Guidelines on Maritime Cyber Risk Management (Cyber Risk Management Guidelines) and adopted a resolution the following year aimed at helping the shipping industry safeguard operations from potential cyber attacks or incidents.

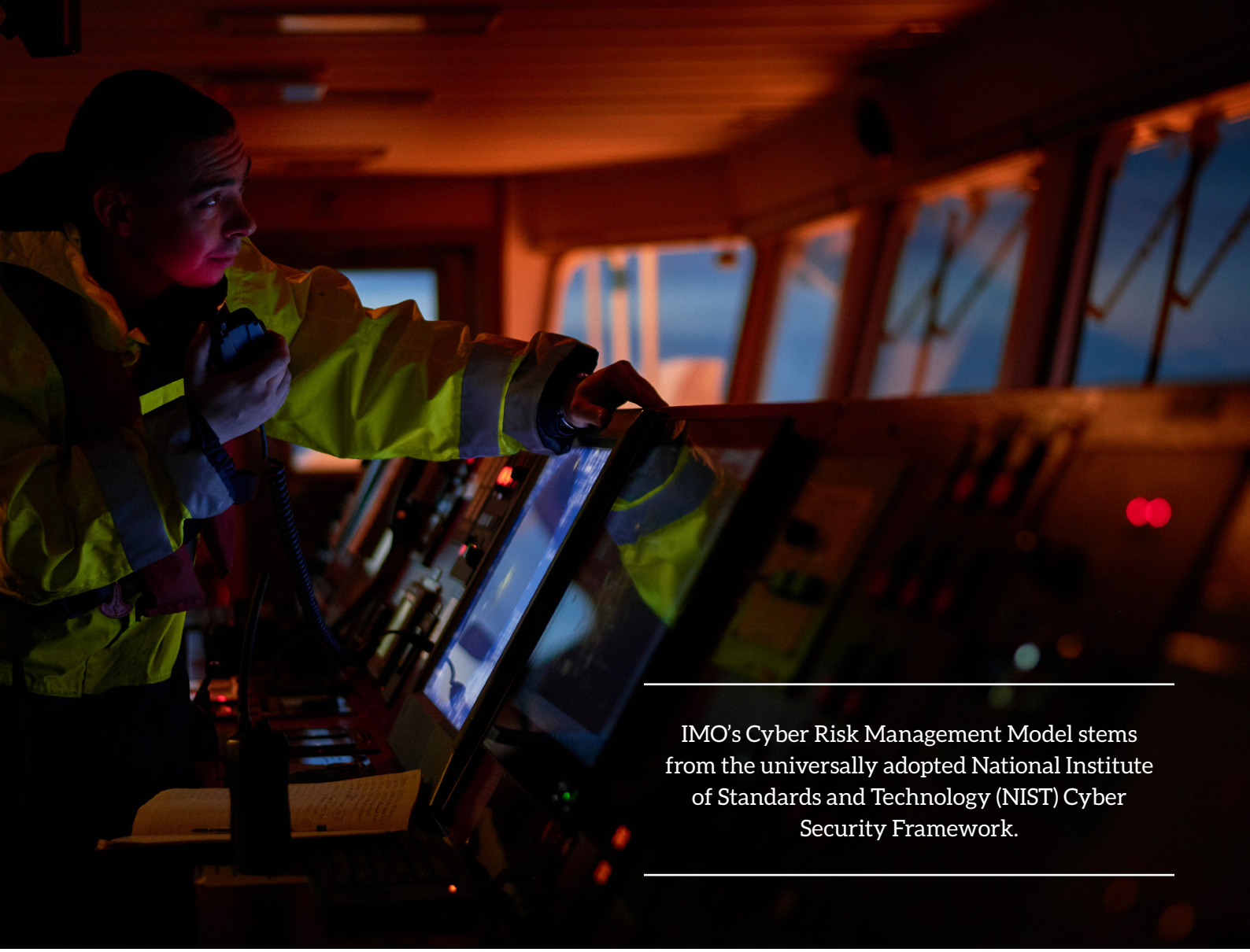
IMO's Cyber Risk Management Guidelines recommend that maritime organizations begin putting into place cyber risk controls and establish cyber resiliency. The IMO resolution recommends for organizations to address cyber risks in their safety management system (SMS) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Essential to Safety and Risk Management

While the 2017 IMO resolution only "encourages" cyber risk management (CRM) compliance, it is important to understand that cybersecurity is essential to your business and critical to the safety, integrity and reliability of maritime assets and operations.

While adopting IMO's proactive guidelines supports effective cyber risk management practices, we recommend that organizations build a comprehensive set of cybersecurity capabilities to facilitate the appropriate levels of conformance with international standards and/or Flag and Port Administration requirements.





IMO's Cyber Risk Management Model stems from the universally adopted National Institute of Standards and Technology (NIST) Cyber Security Framework.

IMO CRM Model

According to IMO, CRM is "the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders."

In addition to the IMO guidelines, a joint industry group including BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL – released the in-depth *Guidelines on Cyber Security Onboard Ships*. This document further supplements the IMO cyber guidelines, risk assessments and defense in depth and breadth, among other elements of conformance.

Updating your SMS will mean understanding and adopting the CRM fundamentals, putting the appropriate level of cyber risk controls in place, building out cybersecurity capabilities and continuously monitoring your overall cyber resiliency in order to prevent, respond to and recover from a cyber incident.

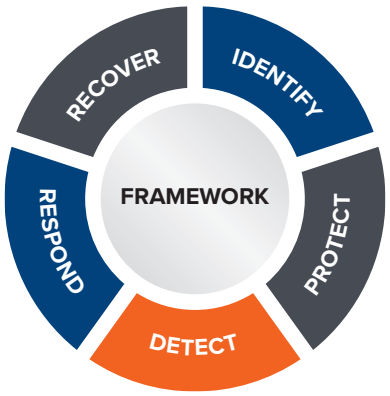


Figure 1 – NIST Cybersecurity Framework

Focusing on the CRM Concept

IMO first defines maritime cyber risk as a measure of the extent to which a technology asset, for example a system on a maritime vessel, is threatened by a potential circumstance or event resulting in shipping-related operational, safety or security failures. That includes information or systems that have been corrupted, lost or compromised due to a cyber incident.

> Cyber Risk Management means the process of identifying, analyzing, assessing and communicating cyber-related risk and avoiding, transferring or mitigating this risk to an acceptable level.

IMO specifies that effective CRM should consider the safety and security impacts resulting from the exposure or exploitation of cyber vulnerabilities in both information technology (IT) and operational technology (OT) systems.

Health, environment, safety and quality programs -- including the SMS -- are well thought out and contain policies and procedures to appropriately manage these risks. Managing safety-related cyber risks requires a deep understanding of the current SMS and the cyber-specific elements to be integrated into the safety program.

IMO's CRM model stems from the universally adopted National Institute of Standards and Technology (NIST) Cybersecurity Framework. The NIST framework provides a clear process model for building cybersecurity programs that references many international cyber best practices from identifying your organization's critical technologies all the way through safely recovering from a cyber incident.

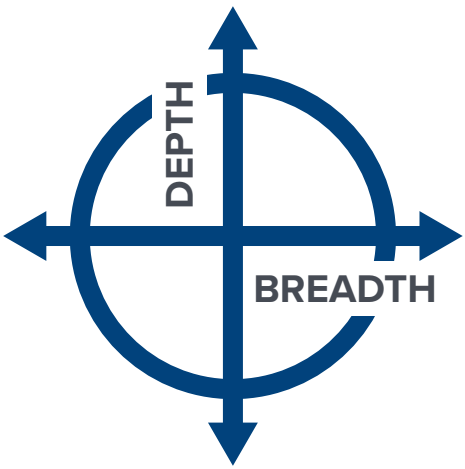
IMO's Guidelines align functional elements that support effective maritime safety, or simply put, best practices needed to implement CRM:

- **Identify** – Define personnel roles/responsibilities for CRM and identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations
- **Protect** – Implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of ship operations
- **Detect** – Develop and implement activities necessary to detect a cyber event in a timely manner
- **Respond** – Develop and implement activities and plans to provide resilience and restore systems necessary for shipping operations or services impaired due to a cyber event
- **Recover** – Identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber event

As such, IMO recommends a risk management approach to cyber risk that is "resilient and evolves as a natural extension of existing safety and security management practices."

Building Cybersecurity Defense in Depth and Breadth

A critical concept the Joint Industry Group emphasizes in its Cyber Security Guidelines is "defense in depth and breadth." What this means at a technical level is three-fold: understanding the necessary actions that must be implemented to establish and maintain an agreed level of cybersecurity, understanding who within the organization is responsible for managing cybersecurity and developing multiple layers of protection and detection measures. Defense in depth is a robust, integrated and layered approach including procedures, policies and technologies, while defense in breadth is meant to cover all the vulnerable cyber technologies—basically a system of systems approach.



The Joint Industry Group states that it is important to protect critical systems and data with multiple layers of protection measures, which consider the role of personnel, procedures and technology to:

- Increase the probability that a cyber incident is detected
- Increase the effort and resources required to protect information, data or the availability of IT and OT systems

Risk Controls	Enterprise	Vessel
Risk Assessments	✓	✓
Training and Awareness	✓	✓
Vendor Risk Management	✓	✓
Management of Change	✓	✓
Incident Response Planning	✓	
Policy Development	✓	
Cyber Architectural Review		✓
Vulnerability Scan		✓
Log Monitoring		✓
Asset Inventory		✓

Risk Controls	Enterprise	Vessel
Incident Response Capability	✓	✓
Risk Management Program	✓	
Data Recovery	✓	✓
Access Controls (IDAM)	✓	✓
Email/Web Management	✓	✓
Vulnerability Management		✓
Patch Management		✓
Intrusion Detection		✓
Whitelisting		✓
Malware Management		✓
Physical Security		✓
Removable Media		✓
Asset Management		✓

Figure 2 – ABS Group recommends the above cybersecurity controls for IMO compliance.

The Joint Industry Group emphasizes that connected OT on board should require more than one technical and/or procedural protection measure. Through a defense in depth and breadth approach, a ship owner would then be encouraged to consider a combination of protection and detection layers ranging from the physical security of the ship in accordance with the ship security plan to network protection and intrusion detection, through to periodic scanning/testing and procedural activities related to cybersecurity controls.

Defense in Depth and Breadth guidance requires that you develop a comprehensive set of security measures otherwise known as controls.

Critical Activities to Build or Enhance Your Cybersecurity Program

Developing a CRM program is more than procedures and policies, it's the implementation and management of technologies. CRM topics and capabilities align with multiple SMS (ISM Code) sections. The right solution for each organization will be different. There will be common elements, but it depends on the risk environment. The Joint Industry Group recommends beginning with a risk assessment, and then proceeding to development of a roadmap to develop capabilities that fit their situation.

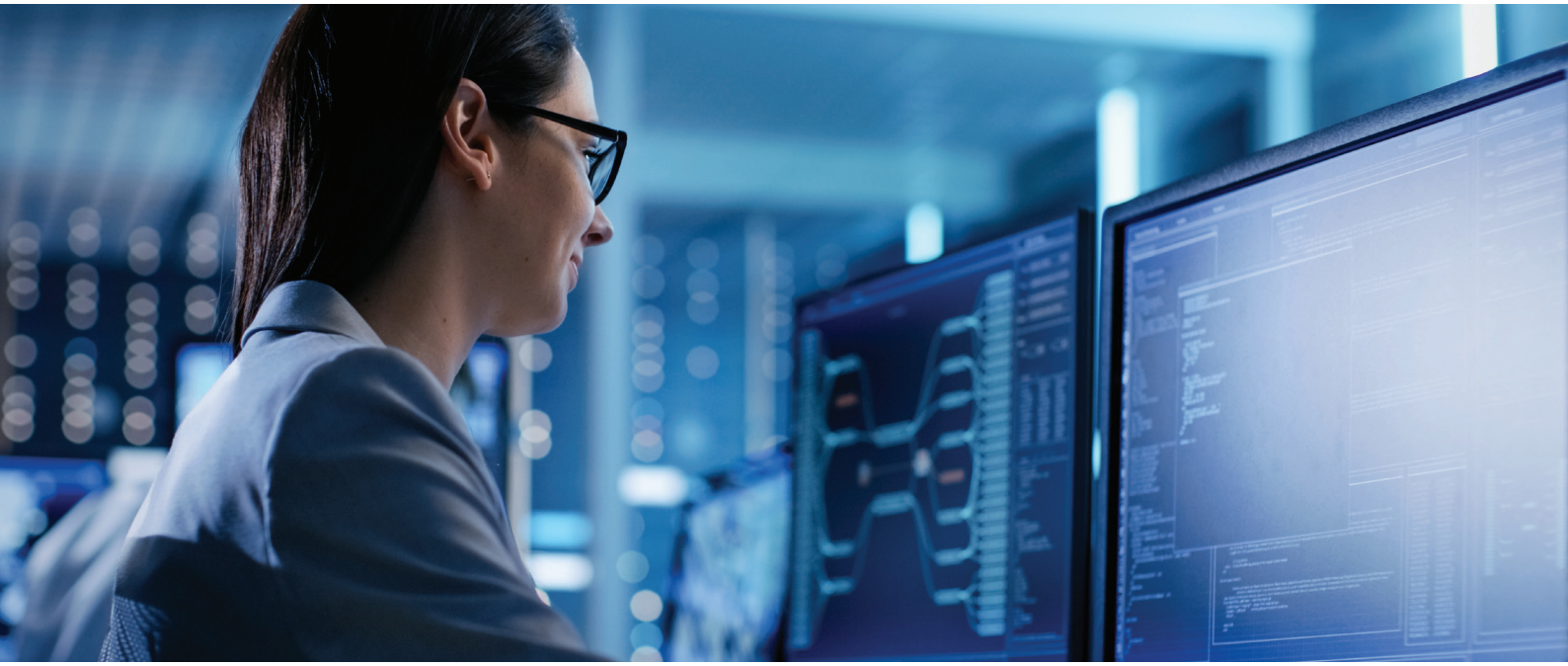
CRM Gap Assessment: Conduct a self-assessment or third-party gap analysis of IMO 2021 preparedness focusing on IMO and the Joint Industry Group against the five key CRM fundamentals: Identify, Protect, Detect, Respond, and Recover

CRM – SMS Road Mapping: Develop a risk-based strategy to update the SMS and build out CRM capabilities in your organization

CRM – SMS Integration: Update your SMS by integrating your CRM policies, procedures and strategies to develop security measures into the program

Security Measure Implementation: Implement a comprehensive cyber program and capabilities to meet IMO guidelines

Most of the effort required to build and maintain cybersecurity capabilities is focused on remediating, mitigating and managing vulnerabilities in critical technologies. Therefore, start by focusing on identifying cyber technologies and vulnerabilities to better understand how to plan and budget for CRM investments.



Identifying Vulnerable Shipboard Cyber Technologies

According to IMO, cyber technologies (critical technologies) have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. Vulnerabilities in these systems could result from inadequate designs, integration and maintenance practices (e.g. human error) or from a lack of technical expertise, capability or discipline related to securing cyber systems within your organization.

Vulnerable OT assets that are increasingly exposed to cyber risk include, but are not limited to:

- Bridge navigation systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Administrative and crew welfare systems
- Communication systems

Because technology is rapidly changing in the maritime industry, and digitalization has become a market reality, the cyber threat landscape is evolving faster than capabilities are being built. This change and uncertainty not only encourage cyber threat actors to take advantage of virtual holes and vulnerabilities, it also makes it difficult for ship owners and operators to address cyber risk only through technical standards.

> "Cyber resiliency is a natural extension of existing safety and security management practices."

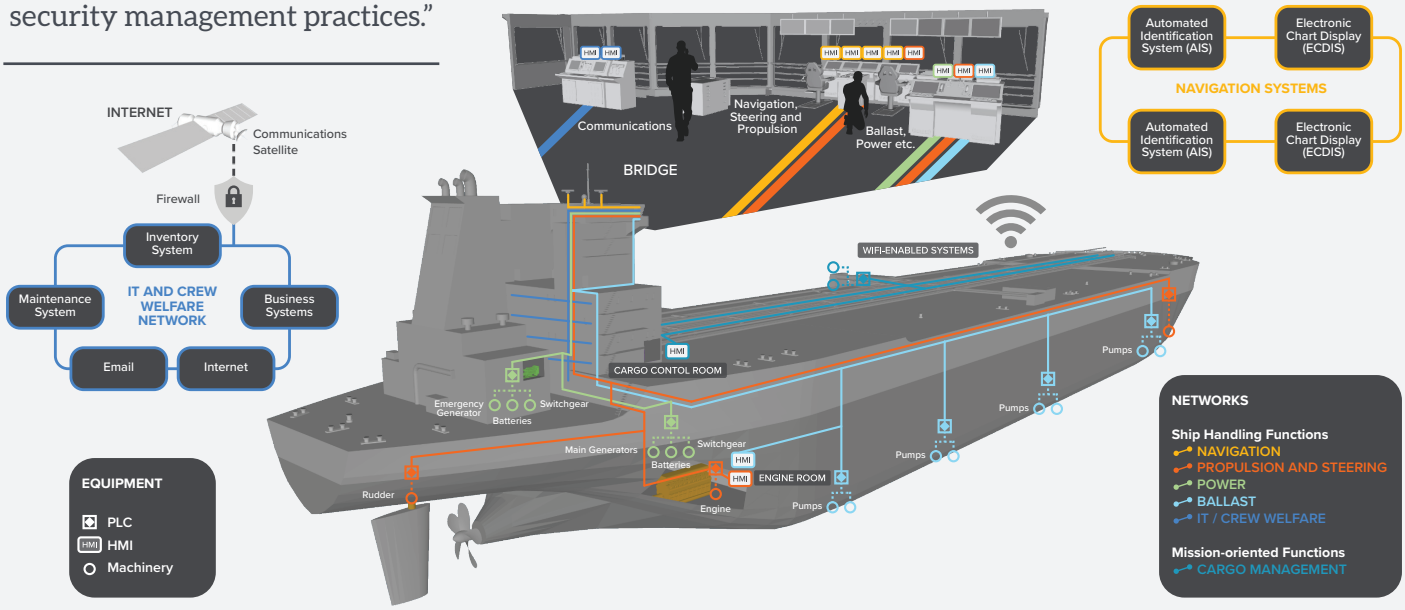


Figure 3 – Vulnerable OT assets increasingly exposed to cyber risk include navigation, propulsion, access control, management and communication systems.

As a practical approach for cyber risk management, the Joint Industry Group recommends identifying what threats and vulnerabilities exist for your organization, assessing your risk exposure, developing protection and detection measures, establishing contingency plans and—should a cyber incident occur—knowing how to respond to and recover from a cybersecurity incident. The Joint Industry Group explains this practical approach as a defense in depth and breadth approach to cyber risk management.

About ABS Group

ABS Group of Companies, Inc. (www.abs-group.com), through its operating subsidiaries, provides data-driven risk and reliability solutions and technical services that help clients confirm the safety, integrity, quality and environmental efficiency of critical assets and operations. Headquartered in Spring, Texas, ABS Group operates with over 1,000 professionals in over 20 countries serving the marine and offshore, oil, gas and chemical, government and industrial sectors. ABS Group is a subsidiary of ABS (www.eagle.org), one of the world's leading marine and offshore classification societies.

cyber@abs-group.com | www.abs-group.com/cyber

About the American Club

American Steamship Owners Mutual Protection and Indemnity Association, Inc. (the American Club) was established in New York in 1917. It is the only mutual Protection and Indemnity Club domiciled in the entire Americas and its headquarters are in New York, USA. The American Club has been successful in recent years in building on its U.S. heritage to create a truly international insurer with a global reach second-to-none in the industry. Day-to-day management of the American Club is provided by Shipowners Claims Bureau, Inc. also headquartered in New York. The Club is able to provide local service for its members across all time zones, communicating in a large number of different languages, and has subsidiary offices located in London, Piraeus, Hong Kong, Shanghai and Houston, plus a worldwide network of correspondents. The Club is a member of the International Group of P&I Clubs, a collective of 13 mutuals which together provide Protection and Indemnity insurance for some 90% of all world shipping. For more information, please visit www.american-club.com.

P&I Insurance

Protection and Indemnity insurance (commonly referred to as "P&I") provides cover to shipowners and charterers against third-party liabilities encountered in their commercial operations; typical exposures include damage to cargo, pollution, death/injury or illness of passengers or crew or damage to docks and other installations. Running in parallel with a ship's hull and machinery cover, traditional P&I cover distinguishes itself from usual forms of marine insurance by being based on the not-for-profit principle of mutuality where Members of the Club are both the insurers and the assureds.

info@american-club.com | www.american-club.com