MSC -DEVELOPMENT OF CYBERSECURITY STANDARDS FOR SHIPS AND PORTS FACILITIES

MSC -DEVELOPMENT OF CYBERSECURITY STANDARDS FOR SHIPS AND PORTS FACILITIES

Submitted by: Team E1

Institute: - COIMBATORE MARINE COLLEGE

Summary:

The provided content highlights the urgent need for robust maritime cybersecurity due to increased digitalization in shipping and port operations, which has made the sector vulnerable to cyberattacks. The IMO's Maritime Safety Committee (MSC) has responded by mandating cyber risk management within Safety Management Systems.

Key suggestions for future IMO sessions include harmonizing rules, developing practical frameworks, improving global compliance, prioritizing technology and crew training, and setting resilience metrics to monitor progress. The summary also calls for mandatory integration of cyber risk into regulatory documents, standardized audit protocols, extended port-specific regulations, supply chain security clauses, the use of AI for threat detection, and continuous incident learning.

The document makes a clear case for binding regulatory amendments, stating that cyber risk is as critical as physical safety measures and must be addressed through enforceable IMO codes. In conclusion, the message stresses the need for holistic rulemaking, regular cyber training, and global collaboration to achieve a resilient and secure maritime sector.

Maritime Cybersecurity: Standards, Compliance & Future Directions

Main Theme

The rapid digitalization of global shipping and ports exposes the maritime sector to escalating cybersecurity threats. Modern reliance on connected technologies (navigation, cargo systems, port logistics) has outpaced legacy safety codes, leaving ships and port facilities vulnerable to cyberattacks. High-profile incidents like NotPetya have revealed the risk to economic stability and operational safety. Recognizing this, the IMO's Maritime Safety Committee (MSC) has initiated global cybersecurity standards—most notably through Resolution MSC.428(98)—mandating that cyber risk management become an integral part of Safety Management Systems (SMS) under the ISM Code.

Relevance for IMO's Next Sessions

Future IMO sessions should focus on:

- ***Rule Harmonization:*** Current guidance is unevenly interpreted and enforced. A unified, MSC-led regulation—flexible but globally auditable—should bridge national and flag-state gaps.

- ***Practical Frameworks:*** Adoption of a comprehensive, goal-based cybersecurity framework (as illustrated in the paper) is needed. This includes mandatory assignment of cyber officers, asset classification, threat/risk assessment, incident response, and periodic crew training.

- ***Global Compliance***: International alignment (with IACS, EU NIS Directives, and classification societies) must be pursued, ensuring standards are robust across both ships and ports. Enhanced certifications and harmonized audit protocols will streamline compliance and minimize disputes.

- ***Technology and Training:*** Encourage cybersecurity-by-design for new vessel builds; require digital retrofitting/planning for legacy fleets. Mandatory cyber-training and regular simulated drills (phishing, ransomware, GPS spoofing) should be specified under STCW updates.

- ***Resilience Metrics:*** Define key performance benchmarks (system patch rates, incident recovery times, annual training targets) for compliance monitoring.

Recommendations for Rule Development & Amendments

- ***Mandatory Integration:*** Cyber risk must be directly embedded in SMS documentation and ISPS security plans, with clear assignment of responsibilities.

- ***Audit Protocols:*** IMO should ensure certification includes cybersecurity controls, incident response practices, and ongoing risk assessments.

- ***Port-Specific Guidance:*** Expand regulatory coverage to address unique operational vulnerabilities and technology dependencies in port infrastructure.

- ***Supply Chain Security***: New clauses are needed to hold vendors and contractors to equivalent cybersecurity criteria.

- ***Digital Twins and AI***: Promote simulation-driven defences and the adoption of intelligent threat detection to future-proof the regulatory landscape.

- ***Incident Learning:*** Formalize post-incident forensics and continuous improvement processes into updated IMO guidelines.

Necessity of Amendments

Cyber risk is a maritime hazard—equal to watertight integrity or navigation safety. The sector cannot continue with patchwork rules and voluntary guidelines. Binding amendments to the ISM and ISPS Codes, plus dedicated IMO recommendations on cyber incident management, will create a level playing field and enable cost-effective, sector-wide resilience. Insurance and liability markets also support minimum global standards to clarify responsibility in the event of a breach.

Requisition to the MSC:

Maritime cybersecurity is now a foundation of modern shipping safety and security. The MSC's leadership, through a harmonized, goal-based, and holistic regulatory strategy, is critical to counter the systemic risks posed by digital threats. The next IMO sessions must prioritize:

- Cementing cybersecurity as a non-negotiable component in all maritime regulations,
- Mandating regular, certified training and incident exercises,
- Ensuring robust checks/audits for both ships and ports,
- for a resilient global transport system able to withstand cyber challenges.
- With global coordination, forward-looking rules, and industry-wide engagement, a secure maritime future is attainable