MARITIME CYBERSECURITY 15 POINT CHECKIST

SHIPUNIVERSE

✅	Step	Key Actions
	1. Conduct a Cyber Risk Assessment	Identify vulnerabilities in IT and OT systems by mapping onboard networks. Assess risks from third-party vendors and the supply chain. Utilize cybersecurity experts or tools to perform a comprehensive analysis.
	2. Develop a Cybersecurity Plan	Create a plan aligned with IMO Resolution MSC.428(98) and the ISM Code. Include risk mitigation strategies, incident response protocols, and contingency plans for critical failures. Integrate the plan into the SMS for operational efficiency.
	3. Crew Training Programs	Train crew to identify cyber threats, such as phishing, malware, and ransomware. Conduct regular onboard drills to simulate handling a cyberattack. Ensure training evolves with new threats and regulatory changes.
	4. Secure IT/OT Systems	Install firewalls, antivirus software, and multi-factor authentication for IT systems. For OT, segment critical systems from the network and ensure regular updates for systems like navigation and engine controls.
	5. Engage Classification Societies	Collaborate with ABS, DNV, or Lloyd’s Register for certifications and compliance assessments. Use their expertise to conduct gap analyses, risk reviews, and ensure adherence to global cybersecurity standards.
	6. Incident Response Protocols	Develop a clear response plan that defines roles and responsibilities during a cyberattack. Include external contacts (IT specialists, flag states) and test data backup systems regularly for recovery readiness.
	7. Monitor and Audit Systems	Conduct vulnerability scans, penetration tests, and system audits regularly. Keep detailed records of these activities to demonstrate compliance during inspections or audits.
	8. Strengthen Supply Chain Security	Evaluate vendor cybersecurity practices and include protective clauses in contracts. Monitor data exchanges with third-party systems, especially with shore-based facilities and port systems.
	9. Comply with Reporting Requirements	Familiarize yourself with reporting protocols under flag state and regional regulations (e.g., USCG, EU NIS2). Establish communication systems for timely reporting and log incidents for future reference.
	10. Invest in Redundancy	Install fail-safe systems and backups for navigation, communications, and propulsion systems. Ensure data is backed up offline to allow recovery even without network access.
	11. Regular System Updates	Keep software, firmware, and IoT devices updated to the latest versions. Apply patches as soon as vulnerabilities are identified to protect systems.
	12. Align with Port Policies	Research and comply with cybersecurity policies for major ports. Establish collaboration with port authorities to ensure smooth operations and avoid delays.
	13. Adopt Cybersecurity Frameworks	Implement trusted frameworks such as the NIST Cybersecurity Framework or BIMCO Cyber Guidelines. These frameworks provide structured approaches to managing cybersecurity risks effectively.
	14. Foster Cyber Awareness	Make cybersecurity a team responsibility by encouraging crew to report suspicious activities. Create a culture where proactive cybersecurity measures are part of daily operations.
	15. Stay Updated on Regulations	Assign a team to monitor changes in IMO, regional, and flag-state regulations. Subscribe to updates from classification societies and maritime authorities for real-time compliance guidance.