



Ships
Cyber Security

Experts in the Operational Technology (OT) that operates the Ship and keeps it safe

Don't risk the safety of the crew, the vessel or its cargo, or pollution

Options available to give different levels of protection and recovery:

- Crew training to reduce human error
- OT & IT protection measures
- 24/7 Monitoring to remote SOC
- Attack Response Plan – be ready
- Navigation & Comms protection
- Restore data & operations
- Facilitate cyber-attack insurance
- Tailor-made Subscription Services

The Threat is Real – the risk of cyber-attack is very high and potentially very damaging. Recent attacks causing major damage affected AP Moller Maersk, Port of Antwerp, BW Shipping and Statoil, with many other incidents not being reported.

Our Team has worked at the highest level in Government Security Agencies and in the maritime industry. We understand the vulnerabilities of IT and have specialist expertise in the Operational Technology (OT) that operates vessels and keeps them safe.

New IMO Regulation: from January 1st, 2021, Cyber Risks must be properly addressed in the ISM Safety Management System.

Networks and Information Security Directive: the NIS Directive is now UK law and mandates essential service providers (including shipping) to take effective cyber security action.

Insurance Exclusions: Institute Clause 380 excludes cover for cyber-attack from marine insurance policies.



Ships Cyber Security

Cyber Prism Delivering Cyber Security Solutions

Cyber Risk & Threat Assessment

- Identify the specific threat vectors
- Document assets to be protected
- Assess consequences of an attack
- Establish risk tolerance and policy

Surveys

- On-board survey of OT & IT systems
- Critical Assets Register & vulnerabilities
- Access controls & data security
- Crew (insider threat) & supply chain

Protection

- Cyber harden survey vulnerabilities
- OT & IT systems protection
- Networks security, eg SHIPGUARD
- Secure Communications & Navigation

Monitoring, Response & Restoration

- 24/7 monitoring for cyber-attack incidents
- Base systems configuration & backup
- Develop Incident Response Procedure
- Restore data & operations expediently

Training & Compliance

- On-board and e-Learning Cyber Training
- Cyber-attack on bridge simulator
- Policies, Procedures incl. Social Media
- Compliance Reviews & Audits

For more information:
www.cyberprism.net
contact@cyberprism.net