



Superyachts Cyber Security

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

Don't risk the safety of the owner, guests and crew or sensitive data breaches

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
- Restore data and operations
- Navigation & Comms protection
- Financial Cyber Crime prevention
- Tailor-made Subscription Services
- Facilitating cyber insurance cover
- Drone counter-measures

The Threat is Real – the risk of cyber-attack is very high and potentially very damaging. Captains are reporting data theft with ransom demands, supplier invoice fraud and interference with the yacht's navigational, comms and operating systems.

Our Team has worked at the highest level in Government Security Agencies and in the maritime industry. We understand the vulnerabilities of IT and the Operational Technology (OT) that operates your yacht.

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

Insurance Exclusions:

Institute Clause 380 specifically excludes cover for cyber-attack from marine insurance policies. We work with Lloyd's underwriters to facilitate cover to be issued with a mix of cyber security options.



Superyachts 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 Asset Register & vulnerabilities
- Access controls & data security
- Crew (insider threat) & supply chain

Protection

- Cyber harden survey vulnerabilities
- OT & IT systems protection
- Networks security, eg YACHTGUARD
- 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 & e-Learning Cyber Awareness Training
- Cyber-attack on bridge simulator
- Policies, Procedures incl. Social Media
- Compliance Reviews & Audits

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