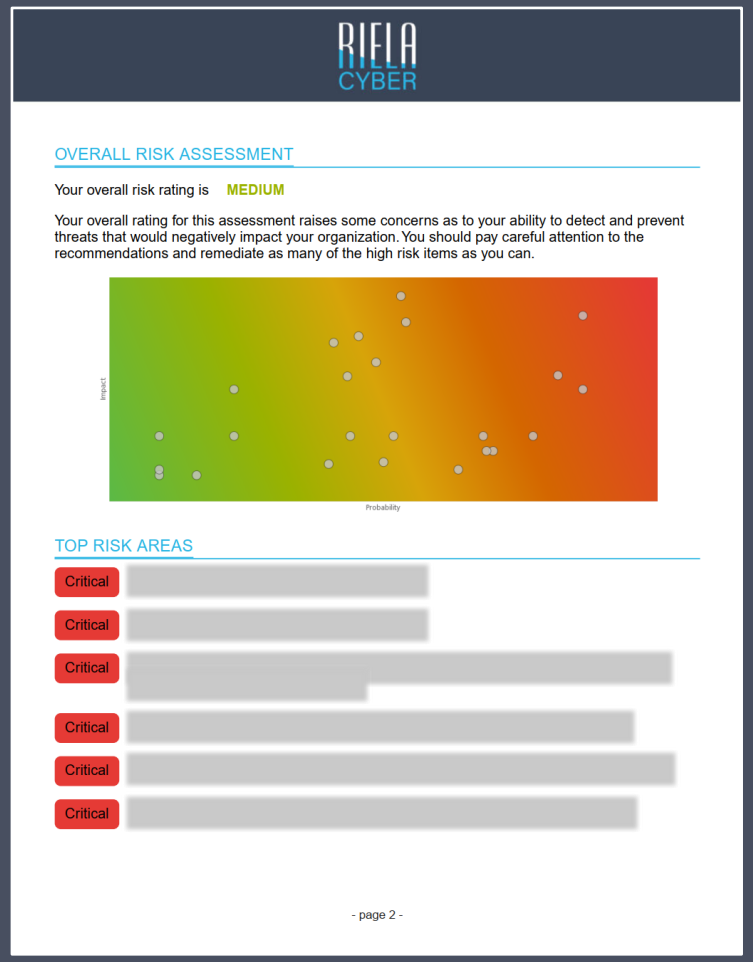
REMOTE CYBER RISK ASSESSMENT FOR YACHTS

RIELA CYBER

- £750
- 1-Hour Remote Consultation
- Dedicated Cyber Security Experts
- Aligned to NIST Framework
- Comprehensive 25-Page Report

RISK POSTURE REPORT
FOR CLIENT REVIEW



RIELA CYBER

OVERALL RISK ASSESSMENT

Your overall risk rating is **MEDIUM**

Your overall rating for this assessment raises some concerns as to your ability to detect and prevent threats that would negatively impact your organization. You should pay careful attention to the recommendations and remediate as many of the high risk items as you can.

Impact

Probability

TOP RISK AREAS

Critical

Critical

Critical

Critical

Critical

Critical

- page 2 -

- Risk Posture Heat Map and Overall Risk Score
- Comprehensive Cyber Security Risk Assessment
- Easy to Understand Results
- Report Delivered Within 24-Hours of Completing the Remote Assessment
- Includes Explanations and Recommendations

NIST CYBERSECURITY FRAMEWORK
OVERVIEW

RIELA CYBER

NIST provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk. The Framework outlines five functions:

1. IDENTIFY
Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risk to ship operations.

2. PROTECT
Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

3. DETECT
Develop and implement activities necessary to detect a cyber-event in a timely manner.

4. RESPOND
Develop and implement activities to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

5. RECOVER
Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

WHY IS NIST IMPORTANT?
IDENTIFY

IMO – INTERNATIONAL MARITIME ORGANISATION
Published MSC-FAL.1/Circ.3 and MSC.428(98) published key documents for "administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders" to "expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities."

BIMCO
Published Cyber Security Onboard Ships (v.3) with further guidelines to enable cyber risk management.

Both the IMO and BIMCO have aligned to the NIST Framework and both encourage to first 'Identify' your cyber risks. It is encouraged that cyber risks are appropriately addressed no later than the first annual verification of the company's Document of Compliance (DoC) after 1 January 2021.

Our Remote Cyber Risk Assessment can help you start by 'Identifying' top level GAP's in your cyber profile onboard. After the report is reviewed, we can work together with you to establish the next steps.

HOW TO PROCEED

CONTACT

Matthew Roberts
matthew@riela-group.com
+44 7425 314 973

RIELA CYBER