CYBER
OWL

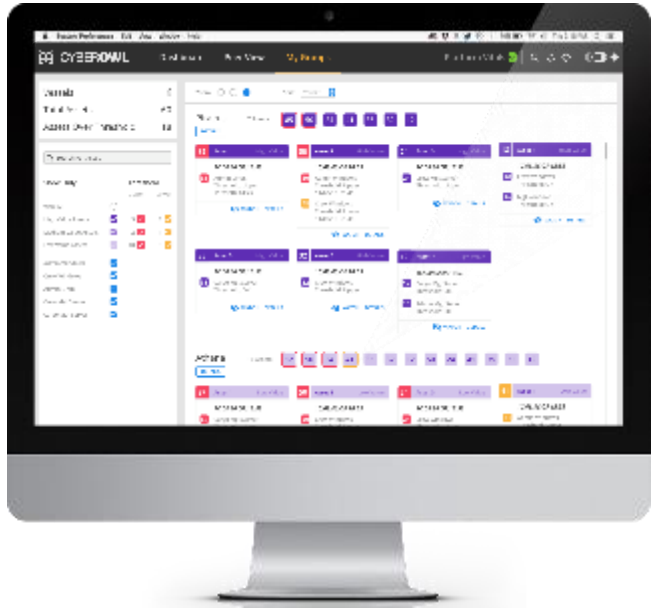
SHIPPING CYBER SECURITY: FEAR, UNCERTAINTY AND DOUBT

Practical cyber security challenges in shipping

CYBEROWL HELPS NAVAL AND MERCHANT SHIPPING PRO-ACTIVELY MANAGE CYBER-PHYSICAL RISKS TO THEIR VESSEL SYSTEMS

INCUS:
Threat detection at "the edge"

MEDULLA:
Cyber intelligence at "the centre"



- **Early warning** of cyber attacks and suspicious crew behaviour
- **Prioritisation** of cyber risks
- **Compliance** with usage policy of vessel IT, IoT and OT

GENERAL OPERATING LANDSCAPE CONTRIBUTING TO CYBER RISK TODAY

- Real focus on sulphur cap in 2020, barely thinking about 2021
- Increasing confidence in the business case for vessel performance optimisation, automation and digitalisation
- Very sensitive to operating expenses
- Crew are getting more technically competent

TYPICAL “SMART SHIP” JOURNEY

- Decisions on technology generally made by marine and electrical engineers, with limited knowledge or consideration for security
- Some level of retrofit or practical workarounds persists, even on newer vessels
- False assumptions are frequently made
- Very limited understanding of software models

REALISTIC THREAT ENVIRONMENT TODAY

- Majority of incidents still relate to poor behaviour, immature policies or non-adherence to policy
- Ransomware and business email compromise is still the main external threat
- Isolated incidents of targeted attacks for now
- Limited no of incidents so far relating to the operational technology, but they have occurred
- Regulation perceived as a threat

MARITIME-EXECUTIVE.COM, 9 JULY 2019

US Coast Guard warns about **malware designed** to **disrupt ships' computer systems**

FLORIDA TREND, JANUARY 2019

Royal Caribbean Cruise Lines face **one million cyber-attacks a day**

HELLENIC SHIPPING NEWS, AUGUST 2019

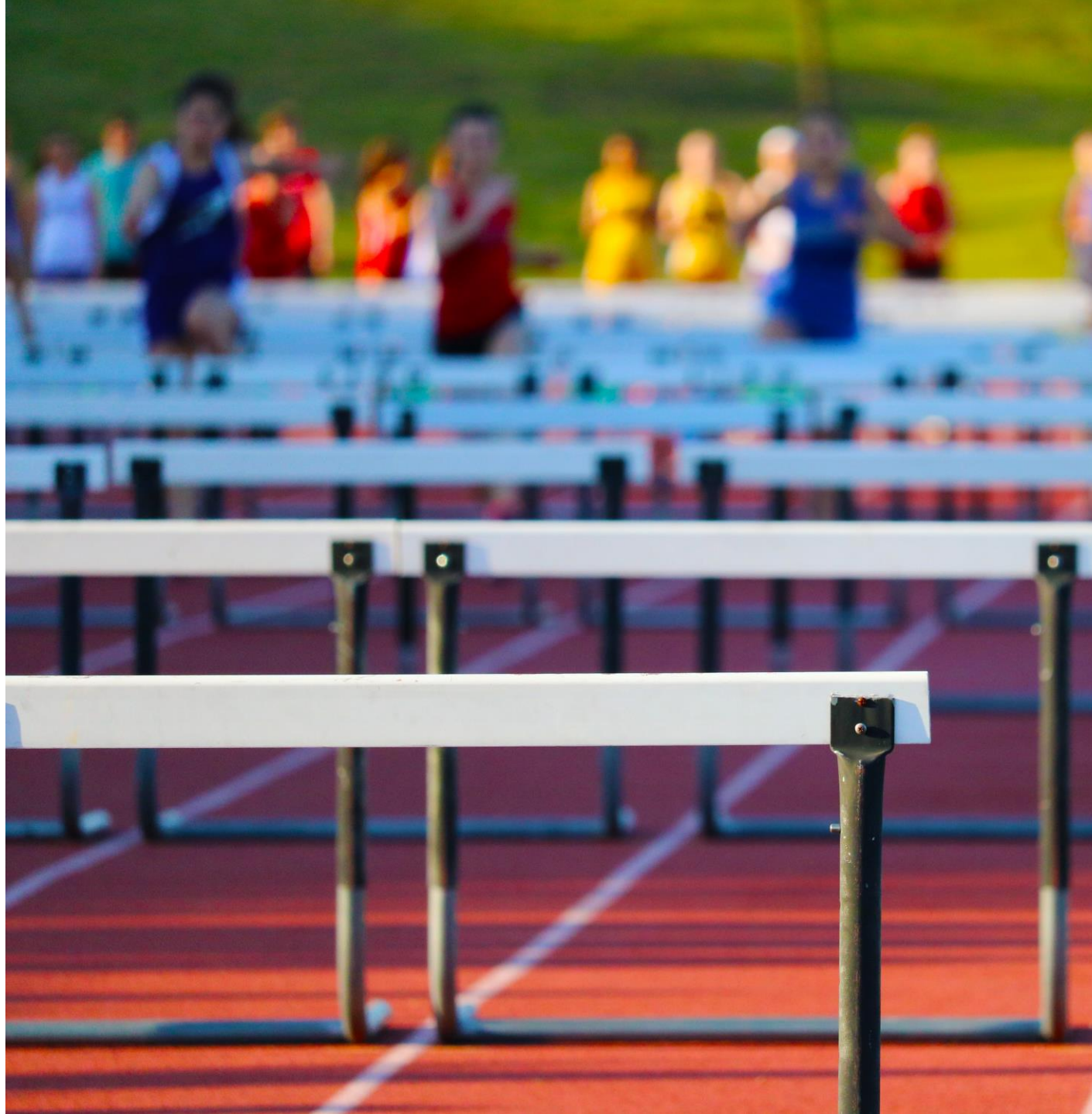
Norwegian National Security Authority advises an **increase** in the number of **cyber attack campaigns targeting maritime sector**

THIS IS TRANSLATING INTO SOME PRACTICAL FOCUS AREAS TODAY

- Zero / minimum visibility e.g. undocumented connected devices, crew behavior, policy deviations
- Demands from auditors / inspectors for evidence of cyber resilience
- Requirement to comply with IMO Resolution MSC.428(98)
- Inspection reports demanding better vessel OT security

THERE ARE SOME CHALLENGES TO ADDRESS GOING FORWARD

- Defining security standards for partial autonomy, particularly on retrofits
- Ownership of the data
- Ownership of the responsibility and liability for cyber security
- A common understanding for measuring the effectiveness of cyber security controls



CyberOwl

www.cyberowl.io
info@cyberowl.io

Registered Address: No. 1 Colmore Square, Birmingham, United Kingdom, B4 6AA