

A guide to IMO2021

What is the new regulation?

IMO2021 regulations state that all commercial vessels over 500 gross tonnage must incorporate measures for addressing cyber risk into their safety management systems, with non-compliance potentially leading to vessel detention.

When was it enforced?

After the first annual verification of the company's document of compliance after 1 January 2021, shipping companies should be following the new IMO2021 regulation.

Why is it happening?

Since February 2020, there has been a 400% increase in cyber-attacks in the Maritime industry. Within an increasingly digital maritime environment, the opportunity for illicit cyber activity has increased and the damage to vessels and shipping companies compounded.



The IMO has suggested that ship operators follow the below framework:

1. Embed a culture of cyber risk awareness into all levels of the organization, starting at the top
2. Comprehensive risk-management objectives and assessments
3. The 5 NIST Cyber Security Framework areas (seen left) should be considered as part of risk management on the SMS
4. All operational systems and their processes / effectiveness should be included
5. A plan to communicate awareness throughout the organization implemented



GCHQ Certified Cyber Awareness Course

Dark Web Scanning

Autonomous End-Point Security Platform

Vulnerability Assessment

- The first cyber security service designed specifically for maritime to protect both vessels and offices
- Establish awareness and create a culture of cyber safety among your seafarers
- Verify that your corporate email domain and any logins associated with it are secure
- Protecting end-points using artificial intelligence, supported by a 24/7 security operations center and full data recovery
- We check for any unsecured devices on your vessels' ICT infrastructure