DBS
DROMON BUREAU OF SHIPPING

clever solutions | beyond class

CIRCULAR

Cyber Risk Management

Following C18049, this Circular wish to draw all parties attention on the updated Guidelines on Maritime Cyber Security.

Notice to: Ship Owners/ Managers/ Operators | Surveyors/Auditors/Verifiers

C22007 | 27 January 2022

Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements.

The IMO Facilitation Committee, at its 45th session, and the Maritime Safety Committee, at its 103rd session, having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved an update to the Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.1).

Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyberdiscipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of

network segregation), there can be implications for security and the confidentiality, integrity and availability of information.

DromonClass Publication

We have updated our Publication on the *Guidelines on Maritime Cyber Risk Management*, which explains to Companies how the cyber risk can be managed through existing Company's implemented procedures. Through our Publication, best practices for implementation are given, that the Company is recommended to use to verify compliance.

Panama Flag Cyber Incident Reporting

The Panama Maritime Authority, aware of the role that maritime transport represents and the risks it faces because of the technological growth on board, wants to encourage all the Panamanian fleet's shipowners, operators, and any other interested parties, to report incidences derived from any cyber event. That will help to better understand the cyber threats to which ships are exposed and implement more effective measures to control such risks.

A voluntary cyber incident reporting scheme has been developed through Merchant Marine Notice (MMN) 22/2021, which is available as of November 17, 2021, on the Ship Registry website.

Act now

ShipOwners/ Managers/ Operators are encouraged to keep records of maritime cyber violation incidents that occur and report them both to Dromon Head Office and the Administration. This will help to better understand and assess the threats to which the ships are exposed and will also contribute to the implementation of a series of protective measures to deteriorate cyber risk in maritime industry.