

Date: 25th November 2020
Circular ref: 2020/MCI/001

Circulated to Insureds, Brokers and Advisory Board Members

CIRCULAR – US to impose tough Port State Control measures on Cyber risk management

Shoreline would like to share the attached news article which appeared in today's Hellenic News. The article relates to heightened [US Port State Controls measures on Cyber risk management](#) which will come into force in line with the 2021 IMO cyber resolution MSC 428(98) on the 1st January 2021.

Shoreline's consultant - Kevin S Cook, Rear Admiral (ret), U.S. Coast Guard - has been keeping abreast of these developments in the US on our client's behalf following a meeting between the USCG and Shoreline's Captain Thomas Brown to discuss maritime cyber related issues in March 2019.

The issue of cyber security insofar as it relates to commercial shipping was highlighted by a case just prior to the aforementioned meeting, in February 2019, when a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network.

An interagency team of cyber experts, led by the USCG, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted.

Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities which could have an impact on the safety of the vessel, port facilities and U.S. waterways.

We believe incidents such as this have prompted the USCG's current port state control posture.

Shoreline is in the fortunate position to be able to assist their shipowner clients with both USCG and IMO cyber compliance by providing the opportunity to purchase Shoreline's [Maritime Cyber Insurance](#) (MCI).

MCI not only provides financial risk transfer it also provides our clients with 24/7 – 365 access to an, expert, global, cyber response service provided by [Charles Taylor Adjusting](#), and, in purchasing the cover, policy holders can avoid the need to pay retainers to any IT specialist service providers.

Consequently, MCI's service offering can support an owner's own planning in respect of two key elements within the BIMCO cyber security model namely:

Response: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event. And;

Recovery: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cybersecurity event.

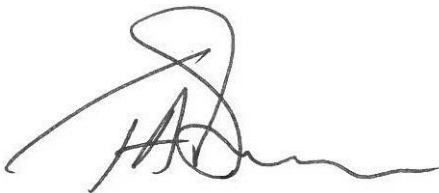
The MCI premium rates that Shoreline can offer their existing clients have been found to be very competitive in a market which continues to harden during the current ransomware pandemic. We are pleased to advise that these rates will be fixed until May 2021.

Very rough pricing indications for limits of cover up to US\$5M can be provided on the basis of fleet size and annual revenue information.

The compliance clock is ticking and Shoreline are ready to assist their clients with their particular cyber insurance requirements.

Please contact the undersigned and or visit our website for more information in this regard.

Yours sincerely,



Captain Thomas Brown
Chief Executive Officer
Shoreline Ltd.
T: +1 (441) 248-0011
E: tbrown@shoreline.bm
W: www.shoreline.bm

Attached Hellenic Shipping News Article

US to impose tough Port State Control measures on Cyber risk management

Hellenic Shipping News 25 November 2020

United States requires all ships, U.S. flagged ships and foreign flagged ships that call on ports in the U.S, to ensure cyber risk management is appropriately addressed in their safety management system by the company's first annual verification of the Document of compliance after January 1, 2021. Failure to this requirement may result in detention of ship in US port.

Members may recall that in June 2017, International Maritime Organization (IMO) at its 98th session of Maritime Safety Committee (MSC) adopted resolution MSC 428 (98), which encourages national administrations to ensure that cyber risks are appropriately addressed in safety management systems (SMS) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

We are not too far from 1 January 2021, and members may receive more detailed information on this from their flag states. Recently United States Coast Guard (USCG) issued information on how they will proceed on ensuring compliance to this resolution.

USCG has instructed their Marine Inspectors (MI) and Port State Control Officers (PSCO) on how to evaluate an SMS and what actions to take in the event of a non-compliance.

The USCG expects that all companies with U.S. flagged ships and foreign flagged ships that call on ports in the U.S. ensure cyber risk management is appropriately addressed in their SMS. In this connection, USCG will include cyber risk assessment in their PSC inspection post 1 January 2021.

If objective evidence is found that the ship failed to implement its SMS with respect to cyber risk management, the following actions may be taken by the PSCO.

1. If cyber risk management has not been incorporated into the ship's SMS by the company's first annual verification of the DOC after January 1, 2021, a deficiency may be issued with action code 30 – Ship Detained, with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.
2. When objective evidence indicates that the ship failed to implement its SMS with respect to cyber risk management, a deficiency for both the operational deficiency and an ISM deficiency may be issued with an action code 17 – Rectify Prior to Departure and require the vessel to conduct an internal audit, focused on the vessel's cyber risk management, within 3 months or, prior to returning to a U.S. port after sailing foreign.
3. When objective evidence indicates there is a serious failure to implement the SMS with respect to cyber risk management that directly resulted in a cybersecurity incident impacting ship operations (e.g. diminished vessel safety/security, or posed increased risk to the environment), the PSCO may issue a deficiency for both the operational deficiency and an ISM deficiency with action code 30 – Ship Detained with the requirement of an external audit within 3 months or prior to returning to a U.S. port after sailing foreign.

In this regard, members are advised to take timely action in ensuring cyber risks are addressed in their SMS and properly implemented on board ships.

Members are also advised that MSC-FAL.1/Circ.3, contains guidelines that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

BIMCO has worked on this subject with other industry partners and produced Guidelines on cyber security onboard ships which is now in its version 3. A new version will soon be out. The Annex 2 of these guidelines may be of specific interest to shipowners as it matches the ISM code with specific cyber risk aspects mentioned in these guidelines.

Furthermore, BIMCO has also published Cyber Security Workbook for On Board Ship Use which is a practical workbook on identifying cyber risks and how to respond in case of a cyber-attack.

Links to the above-mentioned documents

USCG Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) Work Instruction (WI)

[https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-027\(series\).pdf](https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-027(series).pdf)

MSC Res. 428(98)

[https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf)

MSC-FAL.1/Circ.3

<https://docs.imo.org/Search.aspx?keywords=MSC-FAL.1%2FCirc.3>

BIMCO guidelines on cyber security on-board ships

<https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>

BIMCO Cyber security workbook for on board ship use

<https://www.bimco.org/about-us-and-our-members/publications/cyber-security-workbook>