MEMBER ALERT

Shipowners Claims Bureau, Inc., Manager
One Battery Park Plaza 31st Fl., New York, NY 10004 USA
Tel: +1 212 847 4500
Fax: +1 212 847 4599

www.american-club.com

FEBRUARY 2, 2016

CYBER SECURITY GUIDANCE FOR SHIPPING

On January 4, 2016, BIMCO, in collaboration with CLIA, ICS, INTERCARGO and INTERTANKO, published *The Guidelines of Cyber Security Onboard Ships*. This document offers shipowners and operators guidance on how to assess their operations and put in place necessary safeguards and procedures to maintain the security of cyber systems onboard their ships.

As the maritime industry depends more and more on automation and technologies to improve efficiency and reliability, it also introduces an increased threat of security risks due to hacking or sabotage. Cyber-crimes have substantial consequences for shipowners and could potentially compromise safety or lead to environmental incidents. The new BIMCO guidance outlines the key aspects of cyber security and offers a better understanding and awareness for identifying and responding to threats facing the shipping industry.

Reference is made to the BIMCO press release on January 4, 2016 found via the website **here** and the free download of **The Guidelines on Cyber Security Onboard Ships**

Recommended measures

In evaluating their management of information technology, ship operators and owners are advised to consider the following:

- Rather than be delegated to the ship security officer or the head of the IT department, cyber security should start at the senior management level of a company. Initiatives which may heighten security may impose new requirements or policies which ought to be implemented at a senior management level.

- Company cyber risks are specific to the company, vessel, operation and/or trade. Given that cyber threats are constantly evolving, continuous assessment of these risks is essential. A determination of vulnerability should be made by performing assessments of the systems and procedures on board where potential threats may be faced.

- Reducing risk and enhancing defenses are also important considerations. Key information should be protected and kept confidential, and cyber security controls should be put in place.

- Members should develop appropriate contingency plans and conduct regular exercises on board their vessels in order to ensure an effective response to a cyber incident. Additionally, a recovery plan accessible to officers or responsible management personnel and suitable backup systems put in place.

Summary

- Members should approach cyber risks management with the same preparedness required for safety, security and environmental risks already faced.

- All levels of the company, from the senior management ashore to crew onboard, are an inherent part of the safety and security culture within the organization.

- Members should align their policies with existing security and safety risk management requirements contained in the ISPS and ISM Codes and should include requirements for training, operations and maintenance of critical cyber systems.

The BIMCO guidelines provide companies with a risk-based approach to cyber security that is specific to their business and the vessels they operate.

Additional resources

The US Coast Guard now publishes a bi-weekly maritime cyber bulletin to facilitate a greater understanding of the threats and hazards that impact the marine transportation system. These can be found **here** or by going to USCG Homeport – Cyber Security– Cyber News. Also found here are additional US Coast Guard cyber security articles providing recommendations on what shipowners and other companies operating in the maritime industry can do to mitigate the risk of a cyber-attack.

Vessel data recorder vulnerabilities

Members should be advised of recently reported cyber vulnerabilities associated with certain models of Furuno voyage data recorders (VDRs).

An investigation by security researchers at IOActive has revealed that the Furuno VR-3000 (and VR-7000) VDR models may be a hacking target. This vulnerability could allow an attacker with network access to affected devices to execute arbitrary commands with root privileges allowing for the manipulation of data captured on the VDR.

In an effort to reduce such vulnerabilities to hacking and sabotage to VDRs, Members should apply the recommended updates released earlier this month by Furuno:

For VR-3000 and VR-3000S models:

- V1.50 through V1.54 should be updated to V1.56
- V1.61 should be updated to V1.62
- V2.06 through V2.54 should be updated to V2.56
- V2.60 through V2.61 should be updated to V2.62

For VR-7000 models:

- V1.02 should be updated to V1.04

A copy of the Furuno release discussing these software updates can be found **here.**

With this in mind, shipowners are reminded that voyage data recorder systems must adhere to annual performance test requirements, performed by approved service agencies. Performance standards should be well understood and all settings properly configured.

At a minimum, crew should be trained to activate the memory function after an incident in order to prevent the recording over of relevant data. It is important to note that the failure to retain VDR data has serious consequences and could be grounds for significant penalties levied against the owner.

Should Members have any questions or concerns regarding cyber security, they are urged to contact the Managers for further advice and assistance.