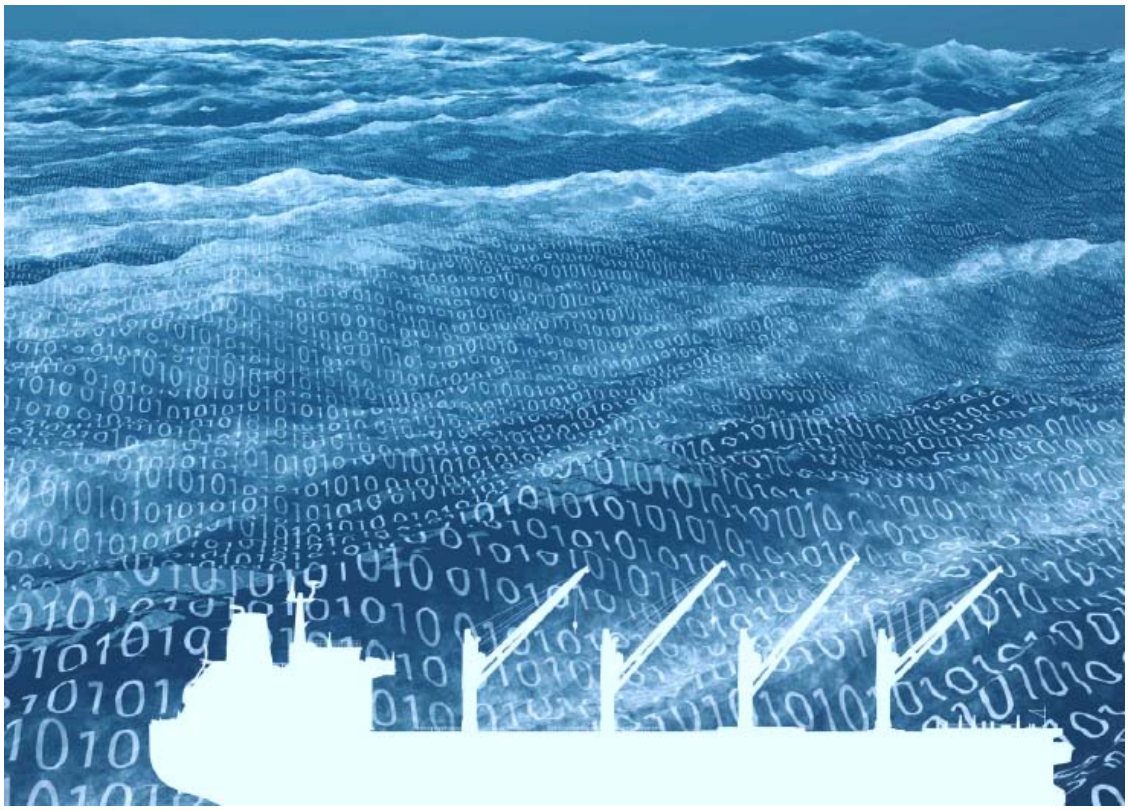

# Gard Alert: Managing cyber risks at sea

Leading shipping organisations have launched a set of guidelines to help the industry prevent major safety, environmental and commercial issues that could result from cyber incidents onboard vessels.

Published 08 January 2016

The " *Guidelines on Cyber Security Onboard Ships* ", developed by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO with support from a wide range of stakeholders, were launched on 4 January 2016. Whilst existing international standards and guidelines on cyber security issues primarily cover shoreside operations, the new guidelines provide guidance to shipowners and operators on how to assess their operations for cyber risks and put in place the necessary procedures and actions to maintain the security of systems onboard their vessels.

The "cyber revolution" is creating new opportunities in the maritime industry – but also new risks and vulnerabilities. The importance of a secure maritime industry is well understood and cyber risks are now becoming a major concern. The guidelines are therefore designed to develop an understanding and awareness of key aspects of cyber security and provide a risk-based approach to identifying and responding to cyber threats.

The new guidelines are free to download from the BIMCO website, click here for a copy of version 1.0.

Managing cyber risks – issues to consider

The maritime industry operates in an internet based computerised environment, and as such, operational risk management is inherently cyber risk management. Shipowners and operators should therefore view cyber risks along with the physical safety, security and environmental risks they already face and establish a "cyber risk management program" adapted to each specific operation/vessel. The following issues should be considered:

• Cyber security is not just an information technology (IT) issue. Thinking of it as simply an IT issue is parallel to thinking about the safe operation of a vessel as simply a main propulsion issue. The risk is operational and cyber security should therefore start at the senior management level of a company instead of being immediately delegated to the Vessel Security Officer or the head of the IT department.
• Cyber security is not only about hackers and attackers. Cyber accidents, such as the unintentional introduction of malware, the improper application of a software patch, or other misuse by well-intentioned employees or service providers can have equally serious consequences.
• All users of IT systems onboard vessels should be aware of the potential cyber security risks, and be trained to identify and mitigate such risks. Initiatives to heighten cyber security levels onboard, both technical and procedural, should therefore be coordinated with tailored crew training and awareness campaigns.
• Every vessel should have access to appropriate contingency plans in order to effectively respond to cyber incidents. Such plans should be available in a non-electronic format and include considerations of methods/lines of communication as well as who has decision-making authority, e.g. when to call in external experts, and whom.
• Periodic tests of contingency plans (exercises) should serve as a means to identify procedures necessary to respond to a cyber incident for inclusion in an existing contingency plan.
• The status of cyber security preparedness of other stakeholders in the supply chain, such as charterers, classification societies and service providers should be ascertained as part of the sourcing procedures for such services.
• Cyber risks are specific to the company, vessel, operation and/or trade and with cyber threats changing all the time, a continuous assessment is vital.

Summary and recommendations

To reduce vulnerability to both cyber accidents and cyber attacks, and ensure safe and efficient vessel operations, Members and clients are recommended to review and address cyber security:

• at all levels of the company - from senior management ashore to the crew onboard, as an inherent part of the safety and security culture onboard each vessel;
• in company policies – align cyber risks with the existing security and safety risk management requirements contained in the ISPS and ISM Codes; and
• in relevant onboard procedures – include requirements to training, operations and maintenance of critical cyber systems.

*Relevant sources of information:*

1) The newly released Guidelines on Cyber Security Onboard *Ships* provides a useful tool for shipowners and operators in their work to assess and manage cyber risks onboard vessels. However, in some cases, alternative risk mitigating methods may have to be used to those suggested by the guidelines in order to comply with all relevant national legislation and flag state regulations.

2) In July 2015, the US Coast Guard published its *Cyber Strategy* in response to what it perceives is one of the greatest threats to US economic and national security interests. The Coast Guard's cyber security website provides access to the strategy document and a variety of other cyber-related information, e.g. their *Cyber Maritime Bulletins* , and can be viewed by using this link: http://homeport.uscg.mil and the following path: Missions > Cybersecurity.

3) In November 2015, DNV GL published a report revealing the top ten cyber security vulnerabilities for the oil and gas industry in Norway. Although the cyber risks picture related to the oil and gas industry may not be directly transferable to the maritime industry, we believe much can be learned from this report. The report can be downloaded from DNVGL's website (the full report is in Norwegian language only).