CYBERSECURITY: THE NEW ENIGMA

THE PERSPECTIVE OF A P&I CLUB

Boriana Farrar

Vice President / Counsel (SCB,Inc.)
Business Development Director- Americas

NOVEMBER 13, 2019

IMO

- IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management.

- The guidelines provide high-level recommendations to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

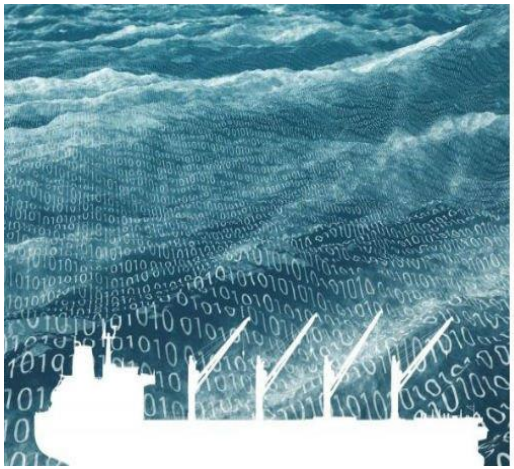
- The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages Flag administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

IMO

- IMO guidelines presented functional elements supporting cyber risk management.
- Identify: To define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
- Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
- Respond: 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.
- Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

- Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI and World Shipping Counsel



BIMCO

- Updated in 2018


Cyber security approach
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to and recover from cyber security incidents
Respond to and recover from cyber security incidents that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

IMO – MSC/FAL Circ. 3 (May 2016)

Guidelines on Maritime Cyber Risk Management **(previously MSC. Circ 1526)**

Establishes high-level guidelines for a holistic, risk management approach to cyber	Aligns with NIST Cybersecurity Framework

IMO – Maritime Safety Committee Resolution 428(98) (June 2017)

Affirms that approved Safety Management Systems should take cyber risk management into account	Encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems by 1 January 2021

Flag State Implementation (June 2017 – January 2021)

USCG collaborating with industry to develop a clear path to compliance with MSC Resolution 428(98)	Development of industry standards, Company implementation, verification, and feedback through the SMS audit process

USCG MARINE SAFETY ALERT: CYBERSECURITY

- The US Coast Guard (USCG) has issued a Marine Safety Alert 06-19: *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels*
- All vessel and facility owners and operators should conduct cybersecurity assessments to better understand the extent of their cyber vulnerabilities:
  - Segment networks
  - Per-user profiles & passwords
  - Be wary of external media
  - Install basic antivirus software
  - Don’t forget to patch
- Marine Safety Information Bulletin (MSIB) 04-19

Department of Homeland Security

- ICS Alerts
- ICS Advisors
- ICS-CERT Monitor Newsletter
- https://www.us-cert.gov/security-publications

P&I Insurance

- IG P&I policies do not specifically identify cyber risks
- A cyber ‘hostile act’ or act of terrorism (a war risk) would be excluded from P&I cover
- FD&D Cover – may be coverage for legal costs & guidance if crime/dispute/loss directly involves an insured vessel

Scenario 1

- Unauthorized access into an agent's email system
- Impersonation of the agent
- Funds directed to impersonator's bank account
- Fraud
- Own economic loss falls outside standard P&I cover
- FD&D
- Learn to spot the red flags

Scenario 2

- Malware is installed by seafarer's mistake (*e.g.* infected USB stick) interferes with its navigation systems and leads to collision, injury, death etc.
- P&I would respond in the normal course
- Training & policies = lead to prevention

Scenario 3

- Compromised monitoring system (known terrorist acknowledges responsibility)
- Falls into war & terrorism exclusion
- Training and policies mitigate risk

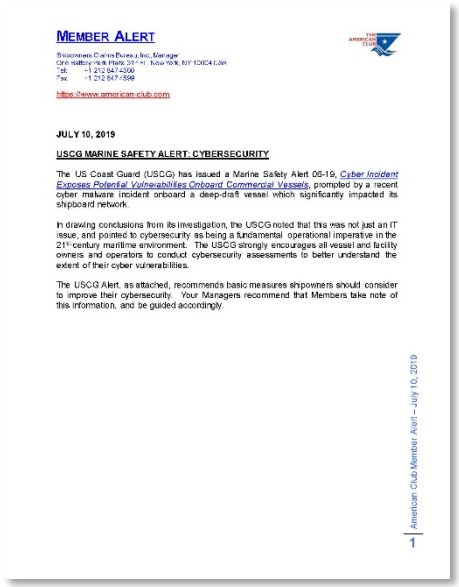
Additional Maritime 'Cyber' Legislation Involving Shoreline Operations

- ISO / IEC 27000 series of standards and guidelines cover shoreside operations, not shipboard
- International Ship and Port Facility Security Code (ISPS) Code related to the risk of the ship / port interface

American P&I Club

- Promoted by The American P&I Club to Members, with reminders of recommended measures
- Member Alert- USCG MARINE SAFETY ALERT: CYBERSECURITY issued 7/2019
- Member Alert- American Club Cyber Security Guidance issued 2/2016:

http://www.american-club.com/files/files/MA_020216_Cyber_Security_Guidance_for_Shipping.pdf



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

https://www.american-club.com

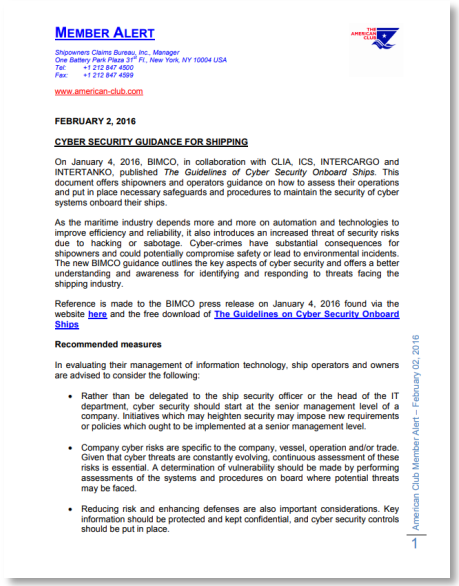
JULY 10, 2019

USCG MARINE SAFETY ALERT: CYBERSECURITY

The US Coast Guard (USCG) has issued a Marine Safety Alert 06-19, *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels*, prompted by a recent cyber malware incident onboard a deep-draft vessel which significantly impacted its shipboard network.

In drawing conclusions from its investigation, the USCG noted that this was not just an IT issue, and pointed to cybersecurity as being a fundamental operational imperative in the 21st century maritime environment. The USCG strongly encourages all vessel and facility owners and operators to conduct cybersecurity assessments to better understand the extent of their cyber vulnerabilities.

The USCG Alert, as attached, recommends basic measures shipowners should consider to improve their cybersecurity. Your Managers recommend that Members take note of this information, and be guided accordingly.



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.

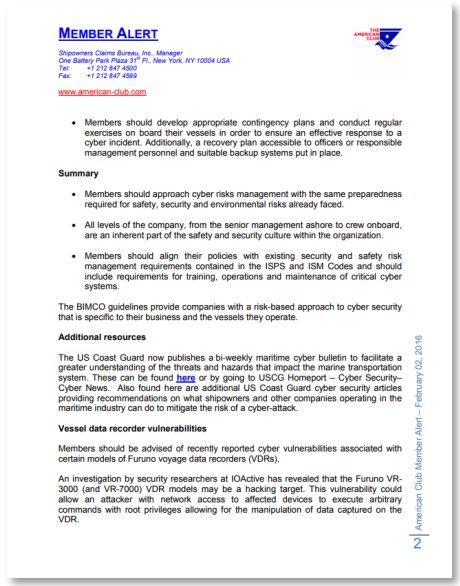
As the maritime industry depends more and more on automation and technologies to improve efficiency and reliability, it also introduces an increased threat of security risks due to hacking or sabotage. Cyber-crimes have substantial consequences for shipowners and could potentially compromise safety or 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.



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

- 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.

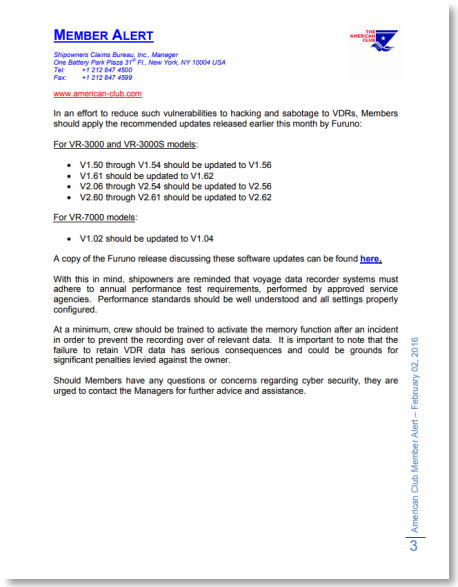
Additional resources

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.



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

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.

Questions?

Thank You!