IUMI Policy Agenda

3. Cyber risks

Brief description

The growing use and reliance on information technology, of data networks, transmissions and connectivity in the daily work within the marine and energy sectors increase their exposure to cyber related risks. Ransomware attacks may result in economic loss or costs of rebuilding lost data. Stand-alone ransomware insurance products are now available both within the marine and non-marine insurance markets to protect against this risk. Consequential damages to hull, cargo and third-party liabilities from a cyber-attack on board a vessel or mobile offshore unit poses a different and more costly risk. The limited data on the frequency, severity of loss or probability of physical damage, is a challenge to underwriters.

The risks can be either malignant or due to innocent breach caused by a lack of awareness or insufficient understanding about systems and how they interact with each other. Both need to be dealt with, starting with top-level commitment and the proper implementation of risk assessment procedures.

Techopedia[1] defines cyber-attacks as deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cyber-crimes, such as information and identity theft. Cyber-attack is also known as a computer network attack (CNA).

A successful cyber-attack can have several implications relevant to insurance: Loss of life, personal injury, pollution, loss of property, business interruption, loss of production, loss of data and loss of reputation. From a cargo perspective, there are in particular concerns related to the potential risks and implications of cyber-attacks directed at unmanned truck convoys and mega hubs.

In December 2016, the USCG published a cyber-security policy letter regarding the criteria and process for the reporting of suspicious activity and breach of security, and added cybersecurity to the list of security items covered by the 2002 Maritime Transportation Security Act (MTSA). This could also mean penalties of up to USD 25,000 per cyber preparedness violation.

[1] http://www.techopedia.com/definition/24748/cyberattack

The EU Network and Information Security Directive (NIS) necessitates amongst others large ports and (static) maritime transport services in the EU to demonstrate that they have taken measures to manage cyber security risks. Companies are also required to report cyber incidents. Penalties for breaches can be substantial, and for instance the UK has announced that firms could face up to GBP 17 million fines if they fail to protect against cyber-attacks.

The International Organization for Standardization (ISO) intends to complement the work on cybersecurity, using the ISO/IEC 27000 series.

IMO

IMO's Maritime Safety Committee (MSC) supported in November 2014 a Canadian / U.S. recommendation to develop voluntary guidelines on maritime cyber security practices. The *"Guidelines on maritime cyber risk management*" were approved in July 2017, and provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. Furthermore, the guidelines refer to additional guidance and standards, including the IUMI supported industry guidelines that are mentioned below.

In June 2017, MSC adopted a resolution on maritime cyber risk management in safety management systems. Member Governments are encouraged to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Industry guidelines

Version 4 of the "*industry guidelines on cyber security onboard ships*" was published in December 2020. IUMI is actively involved in the development, and co-sponsored a proposal requesting IMO's Maritime Safety Committee (MSC) to take the industry guidelines into account when considering measures to enhance maritime cyber security. An update to these guidelines was issued in June 2021.

Unlike other international standards and guidance on cyber security, the industry guidelines focus on the distinctive issues on board vessels. Rather than technical guidance, the guidelines are designed for use by owners, managers and seafarers to develop understanding and awareness of key aspects of cyber security. The company will find support to establish procedures, plans and instructions, including checklists as appropriate, for relevant key shipboard operations that will be complementary to existing security and safety risk management requirements contained in the ISM and ISPS Codes.

In December 2017, BIMCO and Comité International Radio-Maritime (CIRM) presented a proposed industry-wide standard for software maintenance. The International Organization for Standardization (ISO) was approached, and this has resulted in draft standard ISO 24060 that focuses on the concept of a "Ship Software Logging System (SSLS)", specifying requirements for a tool to automatically log all information about software installed on shipboard Operational Technology equipment. If approved, the

standard could serve as a technical tool to support implementation of the CIRM/BIMCO industry standard.

IACS

IACS founded in June 2016 a Cyber Systems Panel. The Panel is focusing on developing recommendations as a first step, to be followed later by new unified requirement on system integration for safety critical shipboard systems. The Panel is also exploring a possible certification scheme for software providers for essential systems by IACS members. An update of UR E 22, covering on board use and application of programmable electronic systems, is under consideration by a project team. IUMI is among the industry partners in a joint working group with IACS on cyber systems.

During September and December 2018, the IACS Cyber Panel published its twelve initial Recommendations addressing; Software maintenance, Manual backup/local control capabilities, Contingency Post Failure, Network architecture, Data assurance, Physical security, Network security, Vessels system design, Inventory list of computer-based systems, Integration, Remote update / access, and Communication and interfaces. In May 2020, IACS published a Single Standalone Recommendation On Cyber Resilience (No. 166), which consolidates the previous 12 recommendations and applies to the use of computer-based systems which provide control alarm, monitoring, safety or internal communication functions subject to the requirements of a classification society.

In 2022, IACS works, mainly through its Cyber Panel together with the IACS JWG on Cyber systems, on the following projects:

1. UR Cyber resilience of ships which shall translate Rec. 166 into an Unified Requirement, publication planned in Q1 2022;
2. UR Cyber resilience of on-board systems and equipment which shall translate Rec. 166 into an Unified Requirement, publication planned in Q1 2022;
3. Establishment of a new Project Team “Data Quality” to develop a recommendation for a generic, superior method/approach on how to determine the data quality required to serve the purpose of a given application, release planned for 2024;
4. Development of an IACS Recommendation on the incorporation of cyber risks into the ISM in order to help shipowners on how to do risk assessment for cyber system and what should be done for mitigation of the risks and to Provide a common framework to carry out risk assessment based on which risk mitigation measures are implemented;
5. Establishment of a new Project Team “Cyber Survey” which aims to develop a new Recommendation or UR about Cyber Surveys;
6. Work on the evolution of the existing UR E22, aiming to finalize the update in 2022.

Industry Standards for Software Maintenance (BIMCO, CIRM, ISO)

The Comité International Radio-Maritime (CIRM) and BIMCO are seeking to propose that IMO develops a resolution or circular on software maintenance, and are in the process of drafting a proposal to MSC 106.

In August 2021, the International Organization for Standardization (ISO) published ISO 24060 (Ships and marine technology - Ship software logging system for operational technology). ISO 24060 was developed by ISO/TC 8/SC 11 and is based on Appendix 5 of the CIRM/BIMCO Industry Standard, and defines a ship software logging system (SSLS) for software installed on a vessel's OT systems. The SSLS maintains an automated software log by monitoring its network connections for software version messages sent by operational equipment. SSLS also stores electronic versions of service reports in association to one or more log entries. This new technical standard is intended to support the CIRM/BIMCO Industry Standard on Software Maintenance of Shipboard Equipment.

In September 2021, BIMCO and CIRM proposed development of the next standard in the ISO 24060 series. In November 2021, ISO/TC 8/SC 1 approved the associated new work item proposal. ISO 24060-2 - Ship software logging system for operational technology - Part 2: Electronic service reports is to be based on Appendix 4 of the CIRM/BIMCO Industry Standard, and will specify a standardised digital format for service reports to be used after finalization of a shipboard software maintenance event, thereby enabling it to be integrated directly with the ship's SSLS and make sure that it is recorded in the onboard software log.

Relevant authority / organisations and documents

- **IMO – Maritime Safety Committee (MSC), Sub-Committee on Navigation, Communication and Search and Rescue (NCSR) & Facilitation Committee (FAL):**
  - ***Resolution MSC.428(98):*** Maritime cyber risk management in safety management systems, adopted 16 June 2017.
  - ***NCSR5/22/4:*** Industry standard on software maintenance of shipboard equipment, submitted by BIMCO and CIRM, 14 December 2017.
  - ***MSC103/9/1:*** The industry guidelines on cyber security on board ships, version 4, submitted by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss, 26 February 2021.
  - ***MSC103/INF.8:*** Update on IACS' work on requirements for cyber resilient ships, submitted by IACS, 26 February 2021.
  - ***MSC-FAL.1/Circ.3/Rev.1:*** Guidelines on maritime cyber risk management, 14 June 2021.
- **United States:**
  - ***Coast Guard:***
    - Guidance on Maritime Cybersecurity Standards, Federal Register/Vol 79, No. 239 12 December 2014 & No. 243, 18 December 2014.

IUMI

        - CG-5P Policy letter: Reporting suspicious activity and breaches of security, 14 December 2016.
        - Navigation and Vessel Inspection Circular (NVIC) 05-17: Guidelines for addressing cyber risks at MTSA regulated facilities, 12 July 2017.
        - Safety Alert 06-19: Cyber incident exposes potential vulnerabilities onboard commercial vessels, 8 July 2019.
    - ***National Institute of Standards and Technology:*** NIST Cybersecurity framework
    - ***US Government Accounting Office (GAO):*** Report on "Maritime Critical Infrastructure protection", June 2014.
- **Be Cyber Aware at Sea**
- **European Union:**
    - ***European Network and Information Security Agency (ENISA):*** Analyses of cyber security aspects in the maritime sector, November 2011.
    - ***EU Directive 2016/1148:*** Concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016.
    - ***TRANSSEC (Transport Resilience and Security Expert Group)***
    - ***European Insurance and Occupational Pensions Authority (EIOPA):*** Cyber risk for insurers – challenges and opportunities, 2019.
    - ***EC DG MOVE:*** Transport Cybersecurity Toolkit, 16 December 2020.
- **IACS:**
    - New UR on system integration for safety critical shipboard systems (under consideration)
    - Certification of software providers under consideration.
    - Revised UR E 22 regarding on board use and application of programmable electronic systems under consideration.
    - Recommendation on Cyber Resilience (No. 166), May 2020.
- **Joint Hull Committee** in conjunction with **Stephenson Harwood:** Cyber risk paper, 2 September 2015.
- **ABS:** Guidance note on the application of cybersecurity principles to marine and offshore operations, Volume 1: Cybersecurity, February 2016.
- **UK Department for Transport & Maritime and Coastguard Agency:** Port cyber security code for operations and staff members, 16 August 2016.
- **DNV:**
    - Recommended practice 0496 – Cyber security resilience management for ships and mobile offshore units in operation, September 2016.
    - Technical & Regulatory News No. 20/2020: ISM Cyber Security is coming soon - check your preparedness, 6 October 2020.
- **International Association of Engineering Insurers (IMIA):** Cyber Risks – Engineering Insurers Perspective, 16 September 2016.
- **Willis Towers Watson:** Client Alert – Navigating cyber risk in the transportation sector, October 2016.

- **BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, IUMI & OCIMF:** The guidelines on cyber security on board ships, 4th edition, 23 December 2020.
- **BIMCO & CIRM:** Industry Standard on Software Maintenance of Shipboard Equipment, Version 1.0, December 2017.
- **The World Association for Waterborne Transport Infrastructure, PIANC Task Group no 204:**
  - Awareness paper on cybersecurity in inland navigation, 2019.
- **Joint Rig Committee** in conjunction with **DNV GL**: Upstream Oil & Gas Cyber Risk: Insurance Technical Review, May 2018.
- **ISO 27001:** International standard for information security management systems (ISMSs).
- **Danish Maritime Authority:** Cyber and information security strategy for the maritime sector 2019-2022, January 2019.
- **FIATA:** Best practices – prevention of cybercrime, 28 March 2019.
- **ClassNK:** Cyber Security Management System for Ships, April 2019.
- **BIMCO:** Cyber Security Clause, 31 May 2019.
- **Digital Container Shipping Association (DCSA):** Cyber security guide, March 2020.

Timeline / important dates

- MSC 98: 7-16 June 2017 – MSC Resolution: Guidelines.
- BIMCO Cyber Security Clause: May 2019.
- IACS: Three new interconnected cyber focused unique requirements, second half of 2021/early 2022.

IUMI will:

- Support the industry guidelines on maritime cybersecurity practices and their implementation, and take part in future revisions.
- Support IACS' work on cyber security, including participation in the Cyber Panel related industry working group.
- Encourage regulatory standardisation for cyber security.