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 needs 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.

According to results from a cyber security survey that was presented by BIMCO, Fairplay and ABS Advanced Solutions in September 2018, more than a fifth of the respondents had been a victim of a cyber related attack. 27% had never received any cyber security training, while only about half of the respondents had a business continuity plan in place.

The United States Coast Guard released its Cyber Strategy guidance document in June 2015. The document presents the agency's vision for operating in the cyber domain and outlines the agency's goals and objectives for its three stated strategic priorities: defending cyberspace, enabling operations and protecting infrastructure. In December

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

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. In mid-July 2017, the USCG announced a request for public comments to its Navigation and Vessel Inspection Circular (NVIC) 05-17: "Guidelines for addressing cyber risks at MTSA regulated facilities".

The EU Network and Information Security Directive (NIS) necessitates amongst others large ports and (static) maritime transport services in the EU to demonstrate 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 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 purpose being to protect and enhance the resilience of cyber systems supporting the operations of ports, vessels, marine facilities and other elements of the marine transportation system. For the purpose of this proposal, cyber security is defined as measures taken to protect cyber systems, or any data contained therein, against unauthorized access, alteration, control, data loss, and prolonged unplanned outage. Cyber systems are defined as any system or subsystem of hardware and/or software whose purpose is acquiring, processing, storing or communicating information or data, including systems that use that data to control physical processes.

In May 2016, MSC approved new *"Interim guidelines on maritime cyber risk management*", providing high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The guideline refers also to additional guidance and standards, including the IUMI supported industry guidelines. In July 2017, the interim guidelines were superseded by an IMO circular informing of the now approved Guidelines on maritime cyber risk management. The industry guidelines below are directly referenced in this circular.

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

In January 2016, an industry group published new "*industry guidelines on cyber security onboard ships*". A 2nd edition of the guidelines was published in July 2017, with the inclusion of among others a new paragraph on insurance cover. IUMI has been 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.

Unlike other international standards and guidance on cyber security, the industry guidelines focus on the distinctive issues on board ships. 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. A revised version 3 of the guidelines will be published in late 2018.

In December 2017, BIMCO and Comité International Radio-Maritime (CIRM) presented a proposed industry-wide standard for software maintenance. The aim is to reduce the number of cyber-attacks on vessels, and the support of organizations and IMO Member States is encouraged. The International Standardization Organization (ISO) has been approached to request the development of an international standard based on the BIMCO/CIRM standard, which may take 3-4 years for completion.

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.

In September 2018, the Cyber Panel published nine of its twelve 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.

e-Navigation

e-Navigation is an IMO initiative defined as “the harmonized collection, integration, exchange, presentation and analysis of maritime information on board and ashore by electronic means to enhance berth to berth navigation and related services, for safety and security at sea and protection of the environment”. To effectively use this as a tool to reduce human error, owners and operators should incorporate e-Navigation Best Practices as an integral part of their Bridge Resource Management (BRM).

The e-Navigation Strategy Implementation Plan, which was approved by MSC 94 in November 2014, contains a list of tasks required to be conducted in order to address five e-navigation solutions, namely

- Improved, harmonized and user-friendly bridge design.
- Means for standardized and automated reporting.

- Improved reliability, resilience and integrity of bridge equipment and navigation information.
- Integration and presentation of available information in graphical displays received via communication equipment.
- Improved communication of VTS Service Portfolio (not limited to VTS stations).

The IMO expects that these tasks, when completed during the period 2015–2019, should provide the industry with harmonized information in order to start designing products and services to meet the e-navigation solutions.

Relevant authority / organisations and documents

- **IMO – Maritime Safety Committee (MSC), Sub-Committee on Navigation, Communication and Search and Rescue (NCSR) & Facilitation Committee (FAL):**
  - MSC95/4/1: Industry guidelines on cyber security on board ships, submitted by ICS, BIMCO, INTERTANKO and INTERCARGO, 5 March 2015.
  - MSC95/4/2: International Ship and Port Facility Security (ISPS) Code cyber security provisions, submitted by Canada, 18 March 2015.
  - NCSR1/INF.5: Background information related to the development of e-navigation, submitted by Norway, 28 March 2015.
  - NCSR1/9: Report of the correspondence Group on e-navigation, submitted by Norway, 28 March 2015.
  - MSC95/INF.19: Cyberphysical relationship in port security – CYSM project, submitted by the European Commission, 14 April 2015.
  - E-Navigation Strategy Implementation Plan, approved by MSC 94, November 2014.
  - FAL40/INF.4: The Guidelines on Cybersecurity on board Ships, submitted by ICS, BIMCO, INTERTANKO, CLIA and INTERCARGO, 30 December 2015.
  - MSC96/4/1: The guidelines on cyber security onboard ships, submitted by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO and IUMI, 4 February 2016.
  - MSC.1/Circ.1526: Interim Guidelines on Maritime Cyber Risk Management, 1 June 2016.
  - MSC98/WP.9: Measures to enhance maritime security, Report of the Working Group, 15 June 2017.
  - Resolution MSC.428(98): Maritime cyber risk management in safety management systems, adopted 16 June 2017.
  - MSC-FAL.1/Circ.3: Guidelines on maritime cyber risk management, 5 July 2017.
  - NCSR5/22/4: Industry standard on software maintenance of shipboard equipment, submitted by BIMCO and CIRM, 14 December 2017.
- **Marsh**: The risk of cyber-attack to the maritime sector, July 2014.
- **IUMI Conference:**

IUMI

  - 2014 – presentation by Markus Wähler, Munich Re.
  - 2015 – President's workshop.
- **United States:**
  - Coast Guard:
    - www.homeport.uscg.mil (Cybersecurity left hand side of page).
    - 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.
  - Symantec Web Security Threat Report 2014.
  - NIST Cybersecurity framework: http://www.nist.gov/cyberframework/
  - US Government Accounting Office (GAO): Report on "Maritime Critical Infrastructure protection", http://www.gao.gov/assets/670/663828.pdf , June 2014.
  - Department of Homeland Security, Coast Guard: Guidance on Maritime Cybersecurity Standards, Federal Register/Vol 79, No. 239 12 December 2014 & No. 243, 18 December 2014.
- **Be Cyber Aware at Sea:** https://www.becyberawareatsea.com/
- **CyberKeel**: http://www.cyberkeel.com/
- **European Union:**
  - European Network and Information Security Agency: 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.
- **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.
  - 9 of 12 recommendations for a cyber resilient vessel, 27 September 2018.
- **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 GL:** Recommended practice 0496 – Cyber security resilience management for ships and mobile offshore units in operation, September 2016.
- **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, 2nd edition, July 2017.
- **BIMCO & CIRM:** Industry Standard on Software Maintenance of Shipboard Equipment, Version 1.0, December 2017.
- **PIANC** – The World Association for Waterborne Transport Infrastructure: WG 204 – Cyber security in inland navigation, established February 2018.
- **Joint Rig Committee** in conjunction with **DNV GL**: Upstream Oil & Gas Cyber Risk: Insurance Technical Review, May 2018.

Timeline / important dates

- IUMI conference Berlin, President's workshop: 16 September 2015 – presentations on maritime industries' draft guidelines and e-navigation followed by a podium discussion.
- MSC 98: 7-16 June 2017 – MSC Resolution: Guidelines.
- 2nd edition of "Industry Guidelines on Cyber Security onboard Ships", 5 July 2017.
- EU Member States to identify operators of essential services within air/railway/water transport by 9 November 2018. Laws and regulations to comply with EU Directive 2016/1148 to be adopted by 9 May 2018.
- NCSR 5: 19-23 February 2018.

IUMI will:

- Support the industry guidelines on maritime cybersecurity practices and their implementation, and take part in future revisions.
- Support IACS' work on the cyber security recommendations, including participation in the Cyber Panel related industry working group, and argue in favour of evolving these into unified requirements.
- Encourage regulatory standardisation for cyber security.