Information Note
No. 1579 – September 2021

Cyber security update

Update on IMO's 2021 Guidelines for Cyber risk Management

Maritime Cyber Security was one of the key themes discussed during the recent London International Shipping Week. According to commentators, there is a cyber incident on a ship every day and attacks on shipping rose 900% in the three years to 2020. Several large container lines have been subjected to cyber attacks and even the International Maritime Organization (IMO) itself has been a victim.

Against that backdrop maritime cyber security awareness on board ships plays an important role in ensuring the safety and security of shipping around the globe and encompasses many factors including commercial risk and key financial exposures, operational and technical issues, compliance, legal implications, in terms of contracts/charterparties, and insurance.

According to IMO, 'Maritime Cyber Risk' refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromise.

From an operational perspective, cyber-attacks can affect the vessel's IT system, OT system and data. For that reason, it is imperative that vessel owners implement cyber security monitoring and have contingency plans in place to deal with cyber breaches.

Members are reminded of **IMO Resolution MSC.428(98)**, 'Maritime Cyber Risk Management in Safety Management Systems' which encourages Flag States to ensure that procedures for the control of cyber risks are included in a vessel's existing ISM Code* Safety Management Systems (SMS). This should be accomplished no later than the first annual verification of the shipowner company's Document of Compliance (DOC) after 1 January 2021. * International Management Code for the Safe Operation of Ships and for Pollution Prevention

Further details are set out within IMO's 'Guidelines on Maritime cyber risk management' (MSC-FAL.1/Circ.3) which were issued in support of Industry in which IMO's Maritime Safety Committee (MSC) and its Facilitation Committee (FAL) jointly approved specific cyber risk management guidelines. For the purpose of the Guidelines, maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

The Guidelines are considered to be a milestone for maritime safety and security, being the product of collaboration between shipping industry leaders and IMO Member States. The ISM Code serves as the foundation upon which IMO Member States have built the 2021 Guidelines for cyber risk management. The IMO encourages Flag States not to issue compliance documents to vessels if cyber risks are not appropriately addressed in the respective safety management system.

The Guidelines provide high-level recommendations for maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities as well as functional elements that support effective cyber risk management.

Through the circular, the IMO recommends vessels and Flag States utilise the guidelines during compliance checks to assess whether cyber risks have been appropriately addressed.

The Guidelines recommend that stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping, including:

- Identifying threats and vulnerabilities;
- Assessing risk exposure;
- Developing protection and detection measure;
- Establishing contingency plans;
- Responding to and recovering from cyber security incidents.

Users of the Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

Members may also wish to refer also to the following guidance and standards:

- *Guidelines on Cyber Security on board Ships* issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss
- *Consolidated IACS Recommendation on cyber resilience* (Rec. 166)
- *IAPH Port Community Cyber Security Report*
- ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

- **Operational Technology** ("OT"): Actual hardware and software monitoring or controlling industrial equipment, assets, processes and events;
  - Examples would be PLCs (Programmable Logic Controllers) and SCADA (Supervisory Control and Data Acquisition) used to gather and analyze data in real-time and monitor or control plant equipment.
- **Information Technology** ("IT"): computer technology, including hardware and software, generally forming the technological backbone of most organizations and companies.
  - Examples would be laptops, personal computers, routers servers, and email and office software.

The two are not completely distinct and are increasingly connected and intertwined.

USCG – recent cyber threats

During August the United States Coast Guard (USCG) issued a note on the Coast Guard Maritime Commons entitled *"Notice of recent cyber threats to the Marine Transportation System".*

It recommended heightened alert as a result of two recent developments. The first was a cyber-attack impacting port operations at container terminals in several South African ports due to *"an act of cyber-attack, security intrusion and sabotage."* The container terminals affected use similar software to that widely used throughout the U.S., and certain processes handled by this software were suspended as a result of the cyber-attack. The attack is believed to be related to the "Death Kitty" ransomware, although full details are still not available.

The second development was the recent release of leaked Iranian documents detailing research into how a cyber-attack could be used to target critical infrastructure. These documents cover research into topics such as how to use ballast water systems to sink a vessel and how to interfere with satellite communications.

Members are encouraged to take action in the following areas:

- Review and ensure that they have appropriate controls in place to protect Operational Technology from cyber threats;
- Review and check Operational Technology infrastructure for potential risks or risky components;
- Closely monitor Information Technology network and system logs for any signs of unusual activity;

- Review incident response plans, security plans, business continuity plans, and disaster recovery plans.

For additional questions relating to this U.S Coast Guard note or to aspects of it relating to the United States, contact maritimecyber@uscg.mil.

For more information, please contact

- For matters relating to HSSE and Maritime security: nick.hough@imca-int.com
- For matters relating to Marine Policy and Regulatory affairs: margaret.fitzgerald@imca-int.com
- For matters relating to digitalisation: andre.rose@imca-int.com