Industry publishes improved cyber guidelines

The third edition of the industry cyber risk management guidelines, Guidelines on Cyber Security Onboard Ships, addresses the requirement to incorporate cyber risks in the ship's safety management system (SMS). It also reflects a deeper experience with risk assessments of operational technology (OT) - such as navigational systems and engine controls - and provides more guidance for dealing with the cyber risks to the ship arising from parties in the supply chain.

"The industry will soon be under the obligation to incorporate measures to deal with cyber risks in the ship's safety management system. This had not been tackled in the previous versions," says Dirk Fry, chair of BIMCO's cyber security working group and Managing Director of Colombia Ship Management.

"The third edition provides additional information which should help shipping companies carry out proper risk assessments and include measures in their safety management systems to protect ships from cyber-incidents. A new dedicated annex provides measures that all companies should consider implementing to address cyber risk management in an approved SMS," Fry says.

"This is much easier said than done", he adds, and notes that the criminals trying to exploit companies or breach their security are getting more inventive by the minute.

The new guidelines are the third edition in as many years, which reflects the constantly evolving nature of the risks and challenges.

OT risks differ

A second key expansion in the guidelines is around operational technology. Ships have more and more Operational technology (OT) which is integrated with Information technology (IT) and which can be connected to the internet, but the risks associated with OT are different from IT systems.

For example, malfunctioning IT may cause significant delay of a ship's unloading or clearance, but with malfunctioning or inoperative OT there can be a real risk of harm to people, the ship or the marine environment.

"On a ship, the job may be less focused on protecting data while protecting operational systems working in the real world has direct safety implications. If the ECDIS system or software controlling an engine are hit with malware, or if it breaks down due to lack of compatibility after an update of software, it can lead to dangerous situations," Fry says.

Another new element in the guidelines is a number of examples of actual incidents to demonstrate some of the real-world situations shipowners and operators face. The examples have been anonymized.

According to the Cyber Security Survey by BIMCO, Fairplay and ABS Advanced Solutions, the joint Industry Guidelines on Cyber Security Onboard Ships, are widely used across the industry. The survey also showed industry is more aware of the issue and has increased cyber risk management training, but there remains room for improvement.

Supply chain risks
A third new focus area is the risk of malware infecting the ship's systems via the many parties associated with the operation of a ship and its systems.

"The ships are not just sitting there in the middle of the ocean. More and more ships are also closely connected to security systems in the companies' offices and shippers' offices and agents' offices," says Fry.

Advice includes evaluating the security of service providers, defining a minimum set of requirements to manage supply chain or third-party risks and making sure that agreements on cyber risks are formal and written.

The guidelines also underline the need for ships to be able to disconnect quickly and effectively from shore-based networks, where required.

The following organisations produced the third edition: BIMCO, InterManager, International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF) and World Shipping Council (WSC).

The work was supported by:
Anglo Eastern, Colombia Ship Management, Maersk Line, Moran Shipping Agencies as well as the cyber security experts NCC, SOFTimpact, Templar Executives and Cyber Keel.

Press contact:
For further information or to request an interview, please contact:

Rasmus Nord Jørgensen
Communications Director
Mobile: +45 2168 0421
Email: rnj@bimco.org

About BIMCO:

BIMCO is the world's largest international shipping association, with around 2,000 members in more than 120 countries. Our global membership includes shipowners, operators, managers, brokers and agents.
As a member, you have access to a wide range of services for free or at a discount.

BIMCO's four core service areas provide value and support to our members:

1. **Products:** BIMCO’s standard contracts and clauses for the shipping industry and our contract editor SmartCon is a key offering to our members. We also run the BIMCO Shipping KPI System which can be used to benchmark ships’ operational performance.
2. **Regulation:** BIMCO takes an active role on behalf of shipowners during discussions and decisions with global and regional regulators and have consultative status at the International Maritime Organisation. We work towards a level playing field for shipping – including fair trade and open access to markets.
3. **Information and advice**: we deal with 10,000 member queries every year via phone or email and see over three million page views on our website each year. Our staff share their expert knowledge on contractual, regulatory and technical matters with members.
4. **Training:** BIMCO conducts face-to-face courses, webinars and tailor-made courses for companies on a variety of shipping related topics.