Cyber compliance and certifications in shipping

A holistic approach with minimal disruptions

Nikolaos Astyfidis, Manager, Advisory Department, KPMG

Eirini Mantzourani, Supervising Advisor, Advisory Department, KPMG

Shipping industry sailing in uncharted waters

The shipping industry is considered the forefront of the supply chain, transporting 90% of the world's trade. As such, the industry faces great challenges, several of which have arisen by the COVID-19 pandemic, whilst others by demanding stakeholders thriving for speed, agility and cost reduction. The need for digitalization is prevailing nowadays, dictating the elimination of paperwork, greater connectivity of devices, adoption of automation and remote monitoring of equipment onboard, as well as remote surveying. As data availability rises, so do requests for accessing vessels' information from different stakeholders: charterers, insurers, agents, ports, equipment manufacturers as well as administration, technical and operation teams shoreside.

While new technologies disrupt and push the maritime sector forward at a rapid pace, cyber security challenges emerge, altering the facade of the global maritime threat landscape. Cyber risk is not only tied to the digitization paradigm, as human and organizational factors must be taken into consideration, in order to ensure business resiliency both at sea and ashore. Attacks aiming the shipping industry have risen more than 900% over the past three years, with 2020 being by far the worst year, incidents-wise, during which a number of major cyber-attacks affected some of the largest global shipping companies.

Regulations and Governance regarding Cyber Security

The IMO having recognized the urgent need to raise awareness on cyber risk to support safe and secure shipping, issued the Guidelines on maritime risk management. The later comprise of high-level recommendations that ought to be incorporated into existing risk management processes and procedures of the shipping companies after January 2021, following the MSC.428(98) Resolution.

Classification Societies in hot pursuit of driving improvement in maritime risk management, are setting new regulations for the certification of cyber secure vessels, considering various important aspects such as technology, procedures, processes, governance and people. All major societies have designed regulations to address both vessels already in service, as well as newbuildings, offering various levels of cyber security certifications depending on the maturity of the shipping company. Moreover, there are also rules aiming at secure vessels by design, which are meant to meet the certification needs of other involved stakeholders, such as shipyards and manufacturers, as well as type approval certificates for cyber secure products, addressing also vendors' requests.
These regulations are aligned - either already or will be in the upcoming future - with the Recommendation on Cyber Resilience (Rec. 166), which was published by the International Association of Classification Societies (IACS) in August 2020. As such, no matter which Society a shipowner chooses as Certification authority, certificates are well recognized by all other major societies coming from a fellow IACS member.

Further to societies, authorities are progressively issuing instructions and checklists to streamline Port State Control (PSC) procedures, with a recent example being the United States Coast Guard (USCG) that launched "Vessel Cyber Risk Management Work Instruction" on 27 October 2020. The instruction contains details and specific focuses to a normal PSC CIC (Concentrated Inspection Campaign) checklist, indicating a general understanding of what PSC inspection on this item would be.

Cyber security compliance: climbing Everest or a walk in the park?

It is, thus, evident that shipowners must consider certifying their fleet according to their requirements

and the security appetite they possess, the soonest possible, so as to address the rising need of cyber secure operations, while ensuring minimal disruption to the daily business during the process.

KPMG has developed pioneering tools tailormade to the requirements of the Maritime industry and several classification societies' regulations, to support shipping companies in their cyber security certification process. KPMG can align to each shipping company's unique requirements and assist throughout the certification process for both IT and OT systems onboard as well as systems at shore, interconnected with the vessels. KPMG possess the knowledge, tools and methodology to gather, or even discover via automated means, all the appropriate information in order to identify the current threat landscape, vulnerabilities and the potential threat actors which might jeopardize the security posture of the company. At this point, should any deviations arise, we have deep knowledge and understanding of the fragile maritime environments as well as best practices in the field to assist the company towards adopting solutions that will strengthen its cyber security posture. Thereafter, we articulate the outcomes to the respective reports required by the Classification society taking into account the regulations' requirements. Finally, upon request, we provide assistance during the certification audit both at shore and onboard, providing the necessary support, throughout the whole lifecycle of the procedure.

KPMG has developed pioneering tools tailormade to the requirements of the Maritime industry and several classification societies' regulations, to support shipping companies in their cyber security certification process. KPMG can align to each shipping company's unique requirements and assist throughout the certification process for both IT and OT systems onboard as well as systems at shore, interconnected with the vessels. KPMG possess the knowledge, tools and methodology to gather, or even discover via automated means, all the appropriate information in order to identify the current threat landscape, vulnerabilities and the potential threat actors which might jeopardize the security posture of the company.

Certifying the vessels alone is a good step towards adopting a cyber security culture at sea, however, shore side information systems, people and processes remain unprotected and vulnerable to an ever-growing threat landscape. Cyber hygiene in the maritime industry should not be limited to vessel's class notations, rather a holistic approach should be adopted to develop organizational culture towards cyber risk management and business resiliency both ashore and onboard. KPMG bringing along years of expertise in the field has a reach portfolio of services to analyse risk and propose secure architectures, train personnel, raise security awareness and perform cyber security incidents' simulations and even assist organizations to respond to events when these occur.

KPMG is, therefore, able to tailor its rich expertise and knowledge to the shipping industry's requirements and transform your journey towards compliance from a cumbersome expedition to Everest into a walk in the park.