Maritime Cyber Security Services

The international shipping industry is responsible for the carriage of around 90% of the world's trade. With the first waves of digitalization starting to hit the sector, new and exciting business opportunities arise. While new technologies disrupt and push the Maritime sector forward at a rapid pace, cyber security challenges emerge, altering the global maritime threat landscape. The omnipresent interconnectivity exposes the sector's infrastructure to ever increasing cyber vulnerabilities and threats. 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.

Maritime cyber security factors

Malware, phishing emails, social engineering, hacking and hacktivism are just few of the actors comprising the global threat landscape that target the maritime industry on a daily basis. Addressing the increasing cyber security challenges requires an active (proactive and reactive) approach, whereby risks are identified and effectively addressed across the three most critical cyber security pillars: human factor, technology and processes.

Human factor

Cyber resilience is highly dependent on individuals. Adversaries tend to easily exploit lack of knowledge and/or awareness for their benefit.

Critical questions to take into consideration:

- How well are your employees trained to resist social engineering?
- Do they have the knowledge and awareness to act upon and adapt to new digital threats?
- Do the Information Technology (IT) & Operations Technology (OT) personnel and the crew communicate efficiently to act swiftly in a time-critical case?

Technology

Digitalization and connected vessels require integration of previously isolated systems and, in most cases, integration with new partners of the digital eco-system. The silver lining in cyber security rests with the appropriate selection of partners to achieve end-to-end results.

Critical questions to take into consideration:

- Are you prepared for the secure integration of IT and OT systems?
- How is your technical infrastructure prepared and tuned for the risk of intrusions from anywhere in the world?
- Did you build in protection mechanisms, and will you be able to detect an ongoing cyber-attack and act upon the relevant alerts?
- Can you isolate and respond to a cyber attack in such a way that the safety of personnel at sea is not jeopardized?

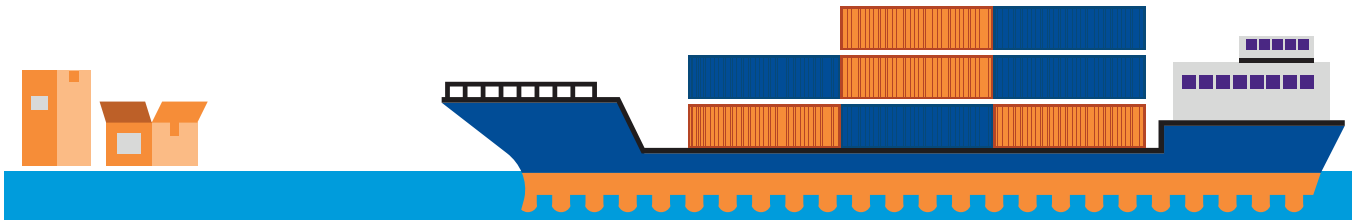
Processes

Organizational changes may be needed so as to be able to reap the benefits of digitalization. While doing so, new processes must support cyber risk mitigation and initiation of the organization's continuity procedures in case of cyber incidents. Cyber threats are cross-sectorial and cross-departmental and are escalated in the presence of organizational silos and lack of proper communication channels.

Cyber threats stemming from digitalization are real. Regulators, like the International Maritime Organization (IMO), have set strict deadlines for ship owners and managers to incorporate cyber risk management into ship safety. Non compliance with these requirements may lead to detention of vessels, signifying financial losses for their owners.

Critical questions to take into consideration:

– How mature is your cyber risk management program?
– Do you have the right tools in place for evaluating and addressing both human, technical and organizational risks?
– Will you be able to prove compliance to upcoming resolutions?
– Can you manage change without greatly affecting everyday vessel operations?



KPMG's Maritime Cyber Security Methodology

KPMG follows a sustained, modular, risk-based approach to help organizations successfully integrate maritime IT and OT equipment and security. We have extensive knowledge of sector standards such as IMO, BIMCO, TMSA, NIST, ISO27001, ISO22301 and experience in various ship classification societies' guidelines and resolutions.

KPMG has been working on securing maritime systems by looking at various important aspects of technology, processes, governance and people. As such, we can adjust our offerings to match the maturity of your organization. We focus on documentation reviews and stakeholder interviews to gather information, supplemented with selected technical spot-checks, whilst using automated means to identify the current threat landscape and vulnerabilities that could be exploited by malicious actors.

KPMG has a deep understanding of the fragility of maritime OT environments. We take special care of health, safety, security and environmental issues and operate with a focus on people's safety and your business continuity.

Cyber risk analysis

– Understand core business requirements and resources.
– Identify internal and external factors and threat exposure.
– Provide tailormade cyber risk analysis for your environment, through the KPMG Cyber Risk Analysis tool.
– Review the sustainability of security governance and compliance monitoring across the organisation.

Awareness and training

– Provide training to personnel.
– Develop easy to follow and to the point material according to role and level of participants.

Penetration testing and vulnerability assessment

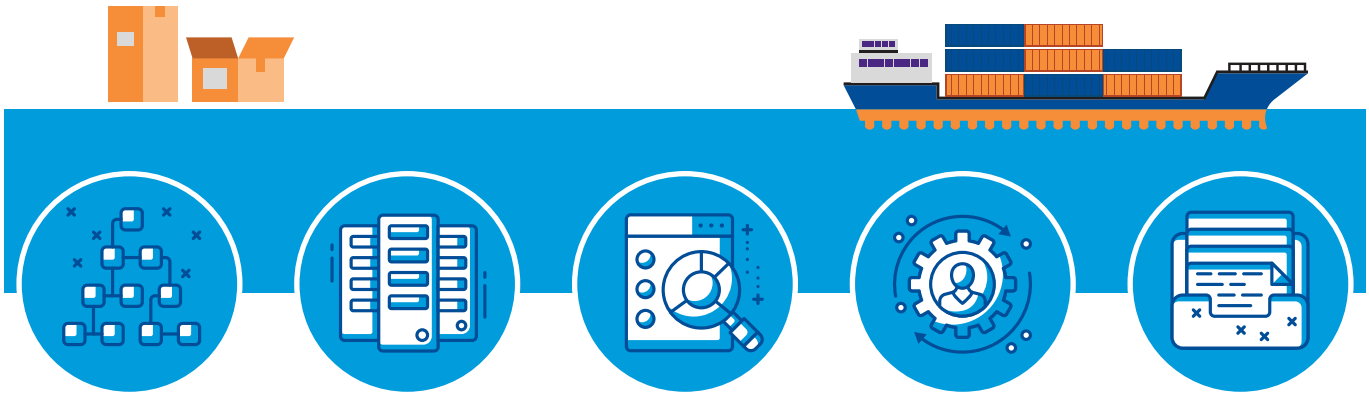
– Identify risks associated with technology and infrastructure.
– Perform social engineering tests as an extra layer of assurance.
– Verify organisation's authentication mechanisms, systems configuration, web services' security, firewalls and sessions.

Monitoring

– Monitor critical systems to identify and counter incidents.
– Ensure that appropriate actions are taken through the relevant incident response teams (CSIRT).

Cyber security incident simulation

– Organise simulation of cyber attacks, based on a range of scenarios.
– Understand organisation's readiness.
– Establish areas for improvement.



Cyber security architecture

- Assess the current architecture (IT&OT) against best practices and international standards.
- Work together to build a tailormade secure infrastructure.
- Propose systems to meet your future security and business needs.

Cyber incident response services

- Rapid response services (emergency response), including KPMG expert opinion, per an agreed SLA.
- 24x7x365 cyber security hotline.
- Post-breach services, including legal assistance and value add services, such as holistic crisis management services and public relations support.

Compliance assessment

- Assess the current compliance state of the organisation against the legal and regulatory requirements.
- Identify gaps and provide guidance for corrective and preventive actions.

Governance

- Build governance framework for information security.
- Determine and articulate your risk appetite.
- Manage your risks effectively.
- Cyber risk reporting in a clear and concise manner.
- Review the sustainability of cyber security across organisation.
- Provide (or review existing) cyber security related policies and procedures.

Classification of marine units

- Provide the appropriate guidance to the organisation in order to achieve cyber security classification.
- Provide the relevant materials (policies, procedures, forms, awareness/training etc.).
- Consultation during the classification processes.

Please get in touch and we will be happy to discuss in more detail.

Efi Katsouli
Partner
E: ekatsouli@kpmg.gr

Nikolaos Astyfidis
Manager
E: nastyfidis@kpmg.gr

Theodoros Stergiou
Director
E: tstergiou@kpmg.gr

e-mail: info@kpmg.gr
kpmg.com/gr

kpmg.com/socialmedia