Expert thinking on critical issues

SAFETY4SEA, in association with the **North of England P&I Club**, discusses topical industry issues.

Q: "Is the industry responding fast enough to cyber risk?"

Cynthia Hudson
CEO,
Hudson Analytix/
Hudson Marine
Management Services

No Owners / managers await regulations, seek a single 'global' solution, have no cybersecurity budget allocated and remain unconvinced about their exposure to cyber risk. Many focus on vessel cyber risk before assessing enterprise-wide cyber security posture; begin instead with understanding, assessment, and then implementation of the cyber security program. Cyber 'maturity' must be measured to be managed, therefore key elements must include benchmarking and continuous improvement. Cargo owners / charterers will require the cyber security stance of chartered vessels. The Owner's BOD, insurers and financial interests need assurance that company assets are protected.

John M. Jorgensen
CISSP-ISSAP,
Chief Scientist,
ABS CyberSafety®

No In light of daily press accounts of cyber attacks by all sorts of players, it is prudent to secure cyber-enabled and safety-related systems and the functions (or assets) they serve. When we automate processes, owners and integrators must understand (and document) the systems they install and use, ensuring they know how these systems can or do affect human, system and ship safety. They need to know the connections these systems have, and who, in crew or not crew, can 'touch' the systems, their data and their functions. Cyber security is not magic, but it is good operations and engineering practices that can enable good business.

Panos G. Moraitis
CEO,
Aspida

Yes At Aspida, we notice a vast difference of the market's understanding of cyber risk today compared to 3 years ago. We consider our industry mature to tackle new risks, and overall its reaction time is faster outweighing the increased risk due to its digitalization. The catalyst was Maersk. Stakeholders realized that cyber risk is tangible with a real effect on operations. Guidelines and maritime cyber security expertise to help owners and operators manage risk are available, while new regulations are incoming. However, there are skeptics believing that cyber risk is fictitious, while others believe that cyber security is a paperwork exercise. Reality will prove them both wrong.

Tero Hottinen
Director, Emerging
Digital Business,
Cargotec Corporation
Management

No In recent years, industries have encountered cases where the focus of cyber attacks has been more towards generating damage to assets instead of focusing on financially or personally sensitive data. Maritime makes no difference here. Publicly reported incidents have created serious discussion and efforts to plug the cyber security holes, but are we fast enough in responding to the risk? Legacy operations and virtually non-existing digital expertise will open up significant threat in case someone really wants to make a massive blast. Yes, we are heading towards more autonomous solutions, but the development is not necessarily going with the first things first – #1 being the safety.

Jostein Jensen
VP Cyber Security &
Data Management,
Kongsberg Digital

No The maritime industry is becoming more connected, but it is not prepared for the consequences of this interconnectedness. As more and more vessels are connecting to the internet, many reap enormous benefits from cross-analyzing data from onboard sensors and automation systems through centralized and cloud applications. This is of great value to the industry, but it comes at a price: vulnerability to most modern cyber threats. Imagine the consequences if adversaries manipulated the propulsion system on a vessel remotely. Although we have seen a shift in awareness and when it comes to cyber security, maritime technology and processes still need to be adapted.

Colin Gillespie
Deputy Director (Loss
Prevention),
The North of England
P&I Club

Yes Change is often said to happen in 3 stages: Awareness, Acceptance and Action. During 2015-2017, awareness of cyber risks was growing in shipping. The notpetya malware attack, at Maersk, along with the growing number of lesser incidents affecting shipping businesses led to an almost universal awareness and acceptance. The industry has quite quickly gone from awareness to the action phase. What is reasonable is to expect owners and their supporting services to be working towards cyber risk management practices. The majority of companies are either already acting or are considering their options and I am confident that the industry can meet this challenge.