cyber attacks on ships. Courtesy: Inmarsat.

Peter Broadhurst is the senior vice-president of safety and security at Inmarsat.

"We have retained the services of Professor Paul Dorey to try and bring the class mindset. Shipping might currently be behind other industries with regards to cyber security, but having their vessel impounded.

The IMO has indeed adopted a resolution telling shipowners and managers they need to abide by certain cyber regulations as it goes from port to port. Government released a comprehensive code of cyber security practices for ships, and political and maritime organisations have also introduced new documentation to build defences.

A recent survey by maritime think-tank Application Technology Global found that 49% of the shipping fleet has experienced a cyber attack in the last 12 months. Current IT defences are not effective at repelling cyber attacks, and that 39% of ships have paid ransoms.

With disasters of this magnitude hitting the headlines, shipping companies are aware of the need to keep ahead of the threat. However, the higher number of systems connected to the internet has boosted the risk of cyber attacks, the effects of which can be devastating.

"The majority of the issues are generated on-board the vessel," says Broadhurst. "It is the crew who are going to be the weak link in the chain. The mindset of maritime is that you build a ship and it lasts fifteen or twenty years, but in reality it needs to be updated. The people in responsible positions are not always as aware of the threats.

"The majority of the crew are generation X or generation baby boomers, and may not be as tech-savvy as they need to be. They don't have the same knowledge of IT, especially if it's not a part of their everyday work."