'Risk of financial loss' prominent in Denmark's new maritime cyber security plan

Mon 21 Jan 2019 by Jamey Bergman

A new cyber security strategy for Denmark has classified financial threats to the maritime sector from cyber criminals and 'government-backed hackers' using ransomware as 'very high' but cyber terrorism threats as low.

The Danish Maritime Authority (DMA) published its Cyber and Information Security Strategy for the Maritime Sector 2019-2022 following a threat assessment from Denmark's Centre for Cyber Security (CFCS).

CFCS' threat assessment concluded that "the general cyber threat against the maritime sector is directed against commercial businesses and does not currently pose a direct threat to maritime operations".

The likelihood of 'destructive cyber attacks' and cyber terrorism in the maritime sector is low, it said, particularly outside of conflict areas.

"Terrorist groups have only shown a limited interest in the maritime sector. Also, terrorist groups lack the capabilities and resources to launch spectacular cyber attacks against the maritime sector," the CFCS assessment said.

Cyber criminals and state-backed actors bent on espionage and blackmail present a far greater risk.

"It is assessed that states systematically use cyber espionage as a means to achieve industrial and business advantages and promote political and economic interests... In particular, there is a considerable threat from cyber criminals aiming to blackmail public authorities, businesses and individuals (ransomware)," the assessment found.

"Networks of cyber criminals exist that are organised and work towards long-term objectives, and cyber crimes are probably also committed by government-backed hackers."

The DMA also commissioned a risk and vulnerability analysis as part of its preparation for the cyber security strategy. Prepared by external consultants, the analysis took in data and dialogue from Denmark's maritime sector, involving the NATO-formed Danish Shipping Board and other public authorities.

Those interviewed for the risk analysis said increased use of information technology (IT) on board vessels had driven up dependency on the systems for core maritime activities and the analysis found private sector maritime players take a 'broad approach' to cyber security.

According to the analysis, the biggest risks to the sector stem from a slow response to technical vulnerabilities, a 'technology gap' between IT systems and operational technology (OT) systems.
such as propulsion, a lack of procedures for ensuring software upgrades and the vulnerability of critical systems to targeted attack.

Consequences from the threats include data loss, data integrity loss, reputational damage and a pronounced risk of financial loss.

Based on the threat assessment, Denmark has put in place a framework of short-, medium- and long-term measures designed to improve the maritime sector's cyber resilience, the first of which was to establish the Danish Maritime Cybersecurity Unit in June 2018.


The maritime sector has been designated as one of the sectors of particular importance to cyber and information security in Denmark. The DMA's cyber security strategy can be found here: [Cyber and Information Security Strategy for the Maritime Sector 2019 - 2022](https://www.marinemec.com/news/view,risk-of-financial-loss-prominent-in-denmarks-new-maritime-cyber-security-plan_56504.htm)