Denmark identifies cyber threats in its maritime sector

Whereas the Danish authorities concludes that the general cyber threat against its maritime sector is primarily directed against commercial businesses, it also emphasises that cyber threats are dynamic and can quickly change.

Published 24 January 2019

Further to our insight " It is time to strengthen your onboard cyber security procedures " of 12 December 2018, the Danish Ministry of Industry, Business and Financial Affairs recently published its Cyber and Information Security Strategy for the Maritime Sector . The strategy is part of the Danish government's national strategy for cyber and information security and contains some interesting observations related to threats, risks and vulnerabilities in the Danish maritime sector.

Although the strategy's primary focus is Denmark, it also addresses cyber attacks aimed at targets outside Denmark. Several Danish shipping companies have a global presence and Danish-flagged ships and their crew have substantial foreign operational and commercial activities. Hence, the following key messages from the strategy may be well worth reviewing, also by non-Danish shipping companies, when incorporating cyber risk management into your safety management system (SMS):

Threat assessment

The Danish strategy concludes that the general cyber threat against the maritime sector is directed towards commercial businesses and does not currently pose a direct threat to maritime operations. In line with the Danish Centre for Cyber Security's (CFCS) Threat Assessment of January 2019, the strategy considers:

• the threat fromcyber espionageto beVERY HIGH. Foreign states can have both financial as well as political interests in conducting cyber espionage against private companies and public authorities;
• the threat fromcyber criminalsto beVERY HIGH. Cyber criminals direct many different types of cyber attacks at private companies and public authorities in the maritime sector. In addition to the economic ramifications, cyber crime may, at worst, disrupt operations in the maritime sector;
• the threat ofcyber activismto beLOW. Cyber activists are typically motivated by ideological or political beliefs and target individuals or organizations they perceive as opponents to their cause. The threat may suddenly increase as hackers can mobilize quickly in the wake of political events and incidents involving the maritime sector, such as transport of controversial goods or oil spills from ships; and
• the threat ofcyber terrorismto beLOW. Even though militant extremists in a few instances have expressed an interest in conducting cyber terrorism, they currently lack the capabilities to do so.

It is, however, worth noting that the assessment is based on the current threat landscape and operates with a warning time frame of 0-2 years and that cyber threats, like other maritime threats such as piracy, are dynamic and can therefore quickly change. Criminals trying to exploit the maritime industry, the ships and their crew are well organised and continuously evolve in the way they operate. This reflects the constantly evolving nature of cyber risk in general.

Risk and vulnerability analysis

In line with the newly published third edition of the industry cyber risk management guidelines the Danish strategy identifies issues related to the integration and compatibility of information technology (IT) and operational technology (OT) systems onboard ships to be a significant risk.

The risks associated with OT systems are different from those associated with IT systems. While a malfunctioning IT system may cause significant delay to a ship's unloading or clearance, disruption of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment, and impede the ship's operation. Despite the potentially severe consequences of a malfunctioning OT, the strategy highlights that there may be a 'technology gap' between the two systems and that shipping companies tend to focus less on maintenance and upgrading of OT systems. It also points to the fact that procedures for upgrading OT systems do not always match the guidelines for IT systems.

Recommendations

In addition to describing several positive initiatives due to be launched by the Danish Maritime Authorities (DMA), the Danish strategy emphasises the importance of:

• consulting relevant international and industry standards and best practices when developing and implementing cyber risk management procedures, whilst ensuring that control measures are adapted to each company's specific risk profile;
• raising awareness of cyber security among all employees. Today, the weakest link when it comes to cyber security is the human factor;
• ensuring that communication, management and guidance on cyber security come from top management. A ship or a department should never act in isolation with respect to cyber security; and
• setting forth specific requirements with respect to suppliers' security level as well as reviewing suppliers' quality performance.

For additional recommendations, Members and clients are referred to our insight It is time to strengthen your onboard cyber security procedures of 12 December 2018.

See also our loss prevention awareness video produced in cooperation with DNVGL.