LNG2026 Qatar قطر 2-5 FEBRUARY

PRESENTED BY IGU INTERNATIONAL GAS UNION UNION INTERNATIONALE DU GAZ GTI ENERGY IIF IIR INSTITUT INTERNATIONAL DU FROID INTERNATIONAL INSTITUTE OF REFRIGERATION

HOSTED BY قطر للطاقة QatarEnergy

Cybersecurity Risk Management Challenges: Maritime Linking the Gas Field to Gas Stove

Lead author: Martin Cartwright, Global Business Director, Gas Carriers & FSRUs, DNV

Co-author: Guillaume Leleu, Senior Consultant, DNV
Svante Einarsson, Head of Cyber Security Advisory EMEA, APAC & Maritime, DNV

As the liquefied natural gas (LNG) industry continues its digital transformation, the complexity and interconnectivity of its supply chain introduce significant cybersecurity challenges. This paper explores the evolving landscape of cyber risk management across the LNG value chain, emphasizing the vulnerabilities inherent in operational technology (OT) and information technology (IT) systems that span geographically and includes interactions of multiple stakeholders on a physical and remote basis over the whole life cycle.

Drawing on recent findings from DNV's Cyber Priority 2025 research, this presentation will examine how the LNG sector is responding to increasing cyber threats with added focus on Shipping, Marine and Port Operations . The maritime segment, which includes LNG shipping and port operations, is experiencing a surge in cyber incidents, with stakeholders identifying cybersecurity as a top operational risk. Similarly, the energy sector is grappling with the dual challenge of securing legacy infrastructure while enabling digital innovation. Both sectors report a growing awareness of third-party and supply chain risks, particularly in procurement and vendor management processes.

Key themes include:

- The fragmentation of cybersecurity responsibilities across the LNG supply chain and its impact on risk visibility.
- The role of regulatory frameworks and industry standards in shaping cyber resilience strategies.
- The need and how to perform integrated risk assessments that encompass both IT and OT environments.
- Case examples of how digitalization initiatives—such as remote monitoring, predictive maintenance, and smart metering—introduce new attack surfaces.
- Strategies for fostering cross-sector collaboration and information sharing to mitigate systemic risks.

This presentation aims to provide a holistic view of cybersecurity risk management in the LNG supply chain, offering practical insights for operators, regulators, integrators, and technology providers. It will also highlight the importance of embedding cybersecurity considerations into the early stages of project design and procurement to ensure long-term resilience.

To view the full technical programme, visit https://lng2026.com/technical-programme

This abstract will be presented during LNG2026 conference on 2-5 February in Doha, Qatar