MANAGING CYBER SECURITY RISKS IN THE MARINE ENVIRONMENT

With vessels increasingly using systems that rely on digitalisation, integration and automation, cyber security risk management is a growing concern in the marine industry. As onboard information technology (IT) and operational technology (OT) is networked together and connected to the internet, the risk of unauthorised access and malicious attacks against a vessel’s systems and networks is growing. It is now more important than ever that vessel owners and operators have a reliable partner with the right know-how to ensure uninterrupted operation and safety.

CYBER SECURITY IN THE MARINE INDUSTRY

The International Maritime Organization (IMO) has recognised that cyber security is becoming critical for data protection and reliable and safe marine operations. In 2017, the IMO adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems (SMS). The resolution stated that an approved SMS should take into account cyber risk management. The resolution also encourages administrations to ensure that cyber risks are appropriately addressed in SMS from 2021 onwards to safeguard shipping from current and emerging cyber threats and vulnerabilities.

OUR SOLUTION

Wärtsilä’s cyber security approach relies on cutting edge technology and industry best practices to safeguard our products and service operations throughout their lifecycle. We help you to develop the resilience required to defend against and recover from any form of cyber interference.

Wärtsilä Cyber services enable you to understand the current cyber security status of your operational environment and provide actions to mitigate identified cyber risks. Our services are designed to give a systematic 360-degree approach to cyber security risk mitigation, from assessing your current cyber posture to implementing cyber controls and lifecycle services.

All Wärtsilä Cyber services are designed according to best practices and are based on the international IEC 62443 cyber security standard. Our services follow guidance on cyber security for the marine industry including:

- BIMCO: Guidelines on Cyber Security Onboard Ships
- ABS: Guidance notes on the Application of Cybersecurity Principles to Marine and Offshore Operations
- DNV: Recommended Practice for Cyber Security Resilience Management
- IMO MSC-FAL.1: Guidelines on Maritime Cyber Risk Management
- IET: Code of Practice, Cyber Security for Ships
Maintaining cyber resilience is a continuous process that should never be thought of as completed. Wärtsilä Cyber services consist of four modules that should be continuously applied to increase your cyber defence.

**WÄRTSILÄ CYBER SERVICES**

- **CYBER ASSESSMENT**
  - Assess your current situation and understand where you are in terms of cyber risks, compliance gaps or technical vulnerabilities.
  - **Wärtsilä ICS risk assessment**
    - Identify your critical assets and understand your related cyber maturity level by revealing cyber risks, possible compliance gaps and technical vulnerabilities.
  - **Wärtsilä ICS vulnerability assessment**
    - Protect your industrial control systems (ICS) and operational technology (OT) environment by identifying and validating security vulnerabilities related to external connections and internal systems.

- **CYBER RECOVERY**
  - Effective incident response is extremely important in the context of cyber resilience. As a leading maritime original equipment manufacturer (OEM) and service provider, we are a right partner for supporting and orchestrating incident response through our PSIRT (product security incident response team) and global service networks.

- **CYBER FOUNDATION**
  - Establish the foundation for your cyber risk management by setting up a cyber security management system, governance and policies.
  - **Wärtsilä ICS security foundation**
    - Establish or improve your ICS cyber security setup by finding the set of policies, standards, industry best practices and rules that best serve your overall risk management strategy.

- **CYBER PROTECTION**
  - We are continuously enhancing the cyber security maturity of our products and solutions in alignment with industry standards (such as IEC 62443) and best practices to reduce cyber risks.
  - **Wärtsilä ICS vulnerability advisory**
    - Receive notifications and guidance on threats and vulnerabilities for specific OT assets along with actionable recommendations to control and mitigate them.
As an OEM and service provider, we have a thorough understanding of the vessel systems and equipment that require securing. We can provide complete lifecycle support to mitigate cyber security risks along with a wide global service network of skilled service engineers, central cyber security experts and strategic partnerships.

Wärtsilä Cyber services are suitable for all marine installations and ports. Delivery is always tailored according to your specific needs and situation, but we recommend starting with a cyber assessment to define your current situation and identify what steps are needed to effectively mitigate your cyber risks.

**YOUR BENEFITS**

- Identify your cyber security risks and understand the actions needed to mitigate them
- Maintain an auditable and managed program to control your cyber security threats
- Ensure preventative protection of your installation against cyber risks and safeguard products and service operations
- Recover quickly and maintain resilience to ensure maximum operational uptime and availability while increasing the reliability of your industrial control system assets