Multi-level Cybersecurity Program

A multi-layered, enterprise-grade approach with integrated hardware and network controls

Managing Cyber Risk in a Connected World

Following an increasing number of high profile and debilitating cyber attacks across the maritime ecosystem, the International Maritime Organization (IMO) adopted Resolution MSC.428(98) to address cyber risks in the maritime industry. The cybersecurity threats that ships face are all too similar to those faced on a daily basis in the office environment. A focus on risk management and the training of crew, together with plans and procedures to identify and deal with a cyber attack, are vital in containing the threat and keeping vessels operating.

IMO 2021 at a Glance

Under IMO Resolution MSC.428(98), also known as IMO 2021, vessel operators are to ensure their existing Safety Management Systems (SMS) appropriately address cyber risks by their 2021 annual verification.

Guidelines generally fall under the U.S. NIST Cybersecurity Framework but a cross-maritime group has extended the framework to assist vessel operators in developing resilient approaches to cybersecurity onboard ships. “The Guidelines on Cyber Security Onboard Ships” has been produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI. See associated framework of the approach below.

Key Requirements:

- Shipping companies need to embed cybersecurity into the culture from senior management to crew
- Shipping companies need to develop and maintain a security management system as part of their SMS
- Companies/vessels must define cyber roles and responsibilities
  - Update SMS policy to include cyber risks
  - Update SMS to include assignment of responsibility for cyber risk management
  - Update SMS and company procedures/training to include cyber risk management

Cyber Risk Management Approach for Vessels

Cyber risk management approach as set out in *“The Guidelines on Cyber Security Onboard Ships”**

Respond & Recover

Respond to and recover from cybersecurity incidents using the contingency plan. Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Identify Threats

Understand the external cybersecurity threats to the ship. Understand the internal cybersecurity threat posed by inappropriate use and lack of awareness.

Establish Contingency Plans

Develop a prioritized contingency plan to mitigate any potential identified cyber risk.

Identify Vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links. Understand the consequences of a cybersecurity threat on these systems. Understand the capabilities and limitations of existing protection measures.

Develop Protection & Detection Measures

Reduce the likelihood of vulnerabilities being exploited through protection measures. Reduce the potential impact of a vulnerability being exploited.

Assess Risk Exposure

Determine the likelihood of vulnerabilities being exploited by external threats and inappropriate use. Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

*Source: bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

KVH's Commitment to Maritime Cybersecurity

Cybersecurity is fundamental to KVH. That's why we employ cybersecurity-by-design principles to the development of our hardware, software, and global communication networks. We offer a variety of features and services to aid vessel operators with their individual cybersecurity needs at onboarding and during regular operations. While each vessel operator remains responsible for ongoing compliance with IMO 2021, KVH's Cybersecurity Program supports those compliance efforts.

KVH's Multi-level Cybersecurity Program

KVH's multi-layer program reduces cyber risk through built-in hardware and network controls.

Integrated Terminal Security

KVH's TracPhone® V30 and TracNet™ terminals include advanced network-level firewall, automated threat management, secure boot, and encrypted drives, and more to maximize terminal security.

Security of Satellite Networks

KVH implements numerous infrastructure safeguards along with different types of authentication and proprietary over-the-air interfaces.

Security of Terrestrial Network

The KVH terrestrial network is designed to separate traffic over the HTS network and to route global satellite traffic over private circuits to MegaPOPs, where Internet egress occurs.

Security Configurations

KVH offers local area network (LAN) segmentation configuration options via firewall, Enterprise extension via VPN, and the ability to enforce login requirements via the versatile mini-VSAT Manager.

Protected Internet Egress

KVH's cybersecurity strategy focuses on protected Internet egress, including: application-level Universal Threat Management (UTM) firewalls in each KVH MegaPOP; application-level traffic shapers; multiple forms of threat detection/blocking; and optional global static IP addresses with all inbound access blocked by default.

Cybersecurity Incident Response

KVH's cybersecurity incident response team addresses threats to the KVH network and is available if a fleet suspects a cybersecurity attack, with the goal to help manage and minimize the risk quickly.

Enterprise-grade KVH Managed Firewall

KVH offers system and network security enhancements using enterprise-grade cybersecurity using the KVH Managed Firewall, powered by Fortinet®. This optional upgrade offers advanced firewall, SD-WAN functionality, intrusion detection/prevention, malware protection, anti-spam, and more.

Cybersecurity for the Future

Resolution MSC.428(98) encourages vessel operators to ensure that cyber risks are appropriately addressed in Safety Management Systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

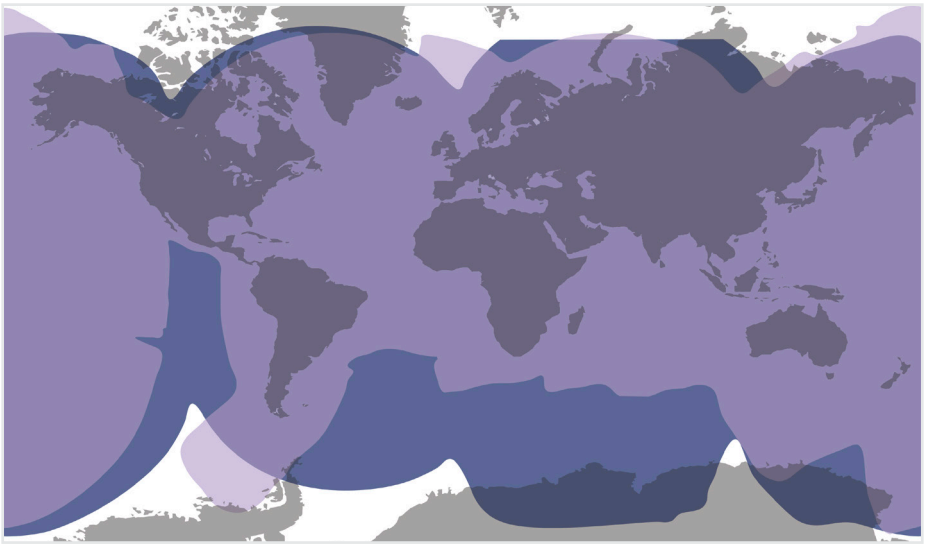
Cybersecurity Ecosystem

Application Engineering: Employing Cybersecurity by Design Principles

KVH's application engineers will work with you to understand your business and technical requirements, anticipate your needs for the future, and help develop a custom network to minimize cyber risks for your fleet and your data. This includes project management, security review and recommendations, documentation, training, and installation of onboard antenna and IT systems. KVH's Application Engineering Team collaborates with your team to determine that the right combination of system elements and configurations has been evaluated, chosen, and specified, to deliver end-to-end solutions that set KVH systems apart from other mobile communications providers.

State-of-the-art HTS Network with Multilayered Network Security

Delivering streaming fast, global, and secure communications for the maritime industry.



Combined Ku- and C-band Coverage

C-band Coverage Only

Ku-band Coverage Only

To view our most up-to-date coverage maps, visit kvh.com/tracnetmaps and kvh.com/htscoverage.

The Superior Choice for Connectivity

Chosen by leading commercial maritime fleets, along with military and government vessels worldwide, KVH's groundbreaking TracNet™ hybrid terminals and award-winning TracPhone systems and global HTS network are relied upon for business-critical operations and communications at sea.

kvh.com/cybersecurity

KVHI NASDAQ LISTED

ISO 9001

World Headquarters
KVH Industries, Inc. · Middletown, RI U.S.A.
+1.401.847.3327 · info@kvh.com

EMEA Headquarters
KVH Industries A/S · Birkeroed, Denmark
+45.45.160.180 · info@emea.kvh.com

Asia-Pacific Headquarters
KVH Industries Pte Ltd. · Singapore
+65.6513.0290 · info@apac.kvh.com

BR_Cybersecurity_0123