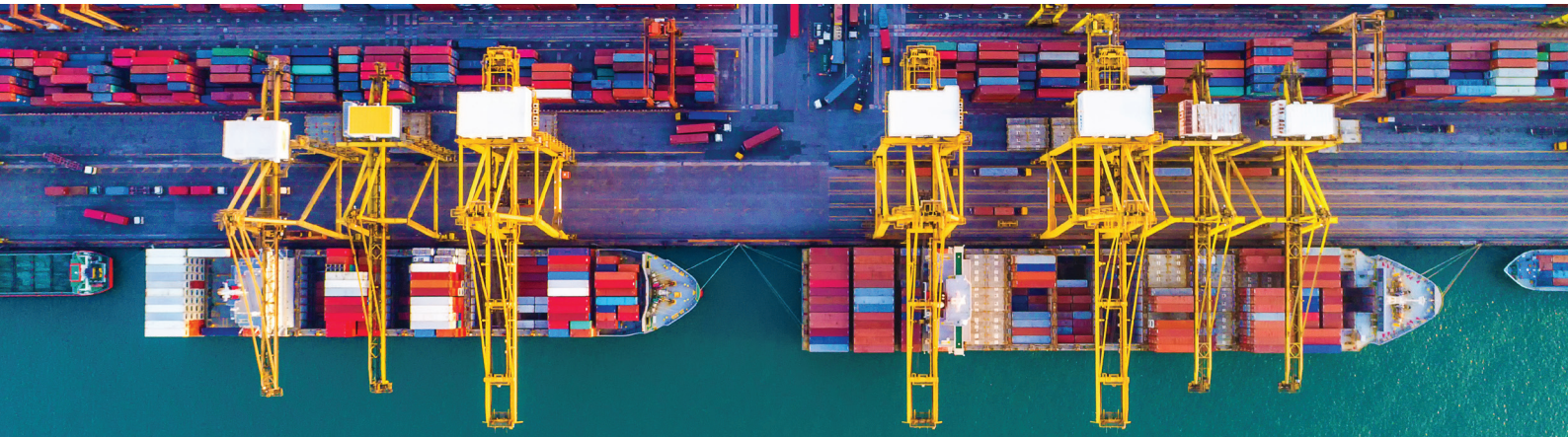
ABS Group



Cybersecurity Requirements for US Port and Marine Terminal Facilities

Recent high-profile cyber attacks have shown that US port and maritime terminals are not immune from this emerging threat. Marine asset/facility owners and operators must now manage cyber risk as well as other major threats, such as physical security, natural disasters and industrial accidents, to maintain safer, more efficient operations. Through our technical advisory services and industry research efforts, we are assisting the marine industry with designing cybersecurity programs, which are tailored to port/marine terminal operations and requirements, in order to facilitate compliance with new cybersecurity policy guidance.

Our marine cybersecurity experts can help plan a course of action to (1) proactively manage cyber risk to your networks and assets and (2) comply with the latest US Coast Guard (USCG) policy guidance. ABS Group has a unique understanding of marine terminals and their associated facilities to provide guidance on a broad range of threats that can impact operations. We apply more than 40 years of experience working with the marine industry and regulators to help contextualize and prioritize cyber threats across the enterprise risk portfolio.

Current State of Cybersecurity

Maritime companies are increasingly concerned with cyber threats, and most have made major investments in information technology (IT) cybersecurity programs to protect confidential data and operation of critical business systems. Far fewer companies are extending their cybersecurity programs to address their operational technology (OT). OT systems, such as industrial control systems or supervisory control and data acquisition (SCADA) systems, detect or cause changes through the direct monitoring and control of physical devices, processes and events.

Historically, OT systems have been isolated from IT networks, but with the rise of Big Data, Data Analytics and the Internet of Things, there are increasing business demands to integrate IT and OT to improve operational efficiency and remain competitive. This opens potential pathways for adversaries (cyber threats) to exploit the cyber domain and achieve their objectives of compromising OT systems.

Read our insights into cybersecurity and managing the risks of integrating IT and OT systems.

Implications of the 2017 USCG Cyber Strategy/Policy

The USCG recognized the emerging cyber threats to its regulated community, and in response, issued new draft guidance in July 2017 for regulated port and marine facilities in an effort to safeguard critical infrastructure and port operations. The USCG Navigation and Vessel Inspection Circular (NVIC) 05-17 titled “Guidelines for Addressing Cyber

info@abs-group.com

www.abs-group.com

ABS Group

Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities," directs regulated marine facilities to include cybersecurity in their Facility Security Assessments and address any vulnerabilities in their Facility Security Plans. Since the plans are focused on reducing risks associated with safety, port disruption and environmental concerns, a traditional IT-centric cybersecurity assessment may not suffice. Rather, a comprehensive approach that assesses IT and OT may be needed.

The policy recommends implementing a cybersecurity program that includes:

1. establishing a cyber risk management team, policies and programs
2. identifying critical systems based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

Guidance for Implementing Cybersecurity Programs

Our cybersecurity experts have experience working with a wide range of cyber security best practices and standards for both IT and OT systems. While we have published our own cybersecurity guidance, our team can help organizations choose the most appropriate standard(s) on which to build their cybersecurity programs based on the nature of their operations. We have mapped the requirements of numerous other standards to the NIST CSF to enable demonstration of compliance with the new policy guidance, including:

- ISO 27001: Information Security Management Standard
- NIST SP 800-82: Guide to Industrial Control Systems Security
- ISA 62443: Industrial Network and System Security
- ABS Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations
- NIST Maritime Bulk Liquids Transfer Cybersecurity Framework Profile
- Control Objectives for Information & Related Technology (COBIT) 5 A Business Framework for the Governance and Management of Enterprise IT

Our Value

As the maritime industry grows increasingly competitive, ports and marine terminals turn to risk management now more than ever for opportunities to improve performance. Leveraging our research and years of experience, we help our port clients assess their exposure to a wide variety of risk – including safety, security, environmental and enterprise – by identifying threats, vulnerabilities and consequences to personnel, assets, operations, critical infrastructure and the surrounding environment. Due to our extensive background in the marine industry working with our parent organization, American Bureau of Shipping (ABS), together with our own risk management expertise, our Safety, Risk and Compliance and Government advisors are uniquely qualified to work with US ports and marine terminal facilities to identify, prioritize and mitigate cybersecurity risk.

ABS Group is leading research efforts on behalf of US government authorities to analyze cybersecurity in the marine industry and build a comprehensive risk framework for US port and marine terminal facilities.

info@abs-group.com

www.abs-group.com

ABS Group