The World's Largest Circulation Marine Industry Publication • The Information Authority for the Global Marine Industry since 1939 • Number 9 Volume 79

MARITIME REPORTER AND ENGINEERING NEWS

MARINELINK.COM

September 2017

Maritime Security

What should be on your radar?

Environmental Regulation
A Hammer Pounding the Waterfront

U.S. Navy
Inside the USS Gerald R. Ford

Port Operations
The Digital Transformation

Voices
Daniel Grunditz, CTO, Chris Marine

Drones
No Longer a Flight of Fancy

FPSOs
New Storage Tank Explosion Frequencies

USCG Releases Draft Cyber Guide for Maritime Facilities

About the Author

James Espino is president of Gnostech Inc. A career Coast Guard Officer, he worked in maritime law enforcement, defense operations, and C4ISR development and procurement.

Cyber risk has hit a critical peak within the maritime industry, and the significant impact of the Petya ransomware attack on scores of maritime entities only amplifies it. The attack effectively shut down major ocean carriers, including shipping conglomerate Maersk, and impacted marine terminal operations across the globe. Every maritime company, no matter the size or business function, is a potential target.

The industry has seen a recent wave of guidelines and resolutions from maritime regulatory bodies related to maritime security and cyber risk mitigation. The International Maritime Organization (IMO)'s Maritime Safety Committee approved a resolution in June that would require ship owners and managers to incorporate cyber risk management into their safety management systems by 2021. BIMCO released the second edition of "The Guidelines on Cyber Security Onboard Ships" the following month. In proper suit, the U.S. Coast Guard (USCG) announced a draft Navigation and Inspection Circular (NVIC) 05-17 entitled "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities" on July 12.

In accordance with existing MTSA requirements, regulated facilities, including port terminals and offshore oil platforms, must identify and assess security threats and develop a Facility Security Plan (FSP) that addresses and mitigates those threats. The USCG has interpreted these provisions to include cyber threats. The NVIC aims to provide guidance on incorporating cybersecurity risks into an effective Facility Security Assessment (FSA), in addition to recommendations for policies and procedures that may reduce cyber risk to operators of maritime facilities. It explains (I) the USCG's interpretation of the existing regulatory requirements under MTSA with respect to cybersecurity measures; and (II) the implementation of a "cyber risk management governance program." While not legally binding, facility operators can utilize this guidance until specific cyber risk management regulations are put into place. Industry stakeholders have until September 11 to provide comments on the draft NVIC.

Enclosure I, "Cybersecurity and MTSA," states that the "existing MTSA requirements are applicable to cybersecurity related threats." The NVIC makes clear that cybersecurity is part of the vulnerabilities assessment and mitigation measures that must be part of existing Facility Security Assessments (FSAs) and Facility Security Plans (FSPs). As with existing MTSA requirements, regulated entities will need to demonstrate how they are addressing cyber risks. The guidance cites existing requirements for FSAs under MTSA to provide structure for the review of the NVIC. Enclosure II, "Cyber Governance and Cyber Risk Management Implementation Guidelines", describes best practices and expectations for all MTSA regulated entities. The guidelines cite the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) to promote effective self-governance.

Cybersecurity challenges are a systemic risk to the maritime industry with the use of cyber technologies for communications, access control and other integrated control systems. Vulnerabilities within these technologies increase their risk for cyberattacks. Attacks targeting industrial control systems (ICS) increased more than 110% in 2016, per IBM. NVIC 05-17 is consistent with the U.S. government's effort to increase private sector preparedness for cyberattacks and reflects a trend towards using a risk management based approach to cybersecurity. It references existing MTSA implementation and its corresponding processes as well as using the NIST framework as guidance for the industry, which is consistent with recently published guidelines.

NVIC 05-17 should take the additional step of detailing specific aspects of an organization's technical implementation of cybersecurity safeguards. This belief is rooted in our company's cybersecurity philosophy consisting of the following foundational pillars:

I. Cybersecurity is an organizational culture that allows technologies to succeed; not a technological solution that results in

Reprinted with Permission from the September 2017 edition of Maritime Reporter & Engineering News - www.marinelink.com

organizational success.

II. A holistic and risk management based systems solution is needed - no single application, tool, or methodology will adequately secure your system.

III. Implement state-of-the-market solutions, but remain current.

IV. A comprehensive maintenance and sustainment program is a critical component of keeping a high cybersecurity posture which minimizes cyber risk.

V. Automate as many processes as you can to minimize human error.

This philosophy is based on our 35 plus years of experience as a technology services provider for the defense industry, in particular improving the security posture of our Navy and Coast Guard customers.

NVIC 05-17 addresses Pillars I and II extensively since cybersecurity is as much cultural as it is technical.

For instance, the guidelines recommend the creation of a multi-discipline cyber risk management team.

Likewise, Pillar IV is somewhat addressed through the need to protect equipment and implement hardware and software updates and obsolesce management programs. However, not enough emphasis is placed on (III) implementing state-of-the-market cybersecurity solutions and (V) automated processes to protect maritime systems. With the understanding that this is a regulatory document versus a technical implementation guide, we believe that incorporating these two items within the regulation can be a catalyst toward reducing long-term cybersecurity costs while at the same time methodically increasing the maritime industry's security posture.

Requiring or recommending the need to implement state-of-the-market solutions to the maritime industry is a step towards eliminating obsolete software and equipment that have contributed to many cyberattacks in recent years. For example, Windows XP is still very prevalent in many industries but particularly for the maritime industry. There are known exploitations within Windows XP and since Microsoft no longer supports this operating system, maritime industry companies still using this operating system are vulnerable to attack. Additionally, state-of-the-market solutions provide all facets of the industry a means to seamlessly and more easily implement NIST CSF into their FSP. Likewise, recommending the use of automated processes for cybersecurity related activities can contribute to reducing a company's long-term need to maintain a robust cybersecurity workforce; thereby, reducing labor costs. Including both state-of-the-market solutions and automated processes within NVIC 05-17 provide the maritime industry the needed guidance to build a robust cybersecurity program within their FSP. This also facilitates implementation of commercially available cybersecurity measures into day-to-day operations, determines a more accurate cyber risk posture, and ensures continuous monitoring of their cybersecurity program vice a periodic snapshot of their cyber risk posture at a given moment in time.

Regulatory bodies across the global maritime ecosystem are increasing their commitment to implement cybersecurity organizations, processes, and systems, and the trend will only continue. NVIC 05-17 is an excellent first step towardsdefining cybersecurity requirements similar to industries such as finance and healthcare. More precise technical cyber recommendations and requirements should be outlined in the same fashion as the organizational and physical security requirements are addressed in this and other regulations.