Maritime Cybersecurity: A Guide for Leaders and Managers

Gary C Kessler & Steven D Shepard (Independently Published, 2nd Edition, 2020), 251

"Maritime Cybersecurity: A Guide for Leaders and Managers," authored by Gary Kessler and Steven Shepard, dissects crucial cybersecurity aspects over nine chapters, aiming to fortify the maritime domain against evolving threats. Gary is a cybersecurity expert with over forty years of experience specializing in maritime cybersecurity and digital forensics. Steven, the founder of Shepard Communications Group, is a tech industry veteran, author, and educator with thirty-five years of experience and a PhD from the DaVinci Institute.

The first chapter offers an in-depth overview of the Maritime Transportation System (MTS), emphasizing its complexity and interdependence across various segments. It underscores the critical need for a holistic cyber defense approach and highlights the diverse stakeholders, significant economic impact, and comprehensive regulatory landscape within the MTS.

The second chapter examines the WannaCry ransomware attack, attributing its origins to North Korea and highlighting its global impact. It emphasizes the urgency of cybersecurity measures by introducing key concepts like the Confidentiality, Integrity, and Availability (CIA) triad, and Parkerian Hexad while advocating for robust cybersecurity defenses.

The chapter explores Advanced Persistent Threats (APTs), highlighting their sophisticated, often state-sponsored nature, with the Operation Aurora cyberattack being a prime example. It also introduces the concept of zero-day exploits as a formidable tool in cyber warfare. While tracing the historical evolution of cyberattack tools since the 1980s, the chapter illustrates their increasing sophistication. It introduces MITRE ATT&CK and NIST Cybersecurity Frameworks, offering practical, structured approaches for organizations to bolster their cybersecurity postures. These frameworks align organizations with best practices and standards, addressing cyber threats' dynamic and complex nature.

The subsequent chapter offers a detailed exploration of real-world cyberattacks in the maritime sector, moving beyond theoretical scenarios. It emphasizes malware threats, mainly focusing on the impact of Stuxnet on Iranian centrifuges. In this chapter, the authors outline various malware distribution methods, including a case study on an oil rig in the Gulf of Mexico. The narrative then shifts to cyberattacks targeting shipping, and highlighting email system compromises at Hyundai Merchant Marine and attacks on Carnival Cruise Lines and Kawasaki Kisen Kaisha (K Line).

Moreover, it explores cybersecurity incidents involving data breaches, such as the compromise of Austal's data management system, the attack on the International Maritime Organization (IMO), and vulnerabilities in smartphone maritime apps like Navionics. It further emphasizes cyber fraud and phishing schemes within the maritime industry, illustrated by notable cases like the fraudulent order of marine gasoil from World Fuel Services and a complex fraud involving Nautilus Minerals, Marine Assets Corporation (MAC), and Fujian Mawei Shipbuilding Ltd. These examples underline the industry's susceptibility to phishing scams and fraud, exacerbated by the high volume of online transactions and communications.

Chapter four emphasizes the crucial role of ports in the global supply chain, acknowledging the system's complexity and interconnectivity. It highlights the supply chain's vulnerability to cyber threats, noting that ports are particularly appealing targets due to their extensive involvement. It also provides real-life examples and discusses proactive measures some port authorities undertake, underscoring the need to address cybersecurity in conjunction with physical security. It concludes by stressing the evolving nature of cyber threats in ports and advocating for united efforts in cybersecurity.

The fifth chapter underscores shipboard security systems' vulnerabilities and susceptibility to cyber threats. It sheds light on specific components crucial for the safety and functionality of maritime operations, including internet-connected cameras, Voyage Data Recorders (VDRs), and communication systems. The later chapter explores the Global Navigation Satellite System (GNSS), including the Global Positioning System (GPS) and Automatic Identification System (AIS), which are crucial for maritime safety and various Positioning, Navigation, and Timing (PNT) applications. Surprisingly, these systems are vulnerable to low-tech attacks by various adversaries. The authors explore the evolution of GPS spoofing, from minor deviations in a single vessel's course to complex manipulations involving multiple vessels, including warships. This underscores the escalating threat and highlights a significant risk in the ongoing battle against vulnerabilities in PNT technologies.

Chapter seven explores the maritime industry's transformative journey towards the future, marked by integrating core technologies, such as the Internet of Things (IOT), operational technology, and autonomous maritime systems. It emphasizes that it is crucial to adopt and adhere to cybersecurity guidelines, such as the SP800-82 Guidelines from NIST and the International Electrotechnical Commission (IEC) 62443 family of standards. These provide a foundational framework for securing Industrial Control Systems (ICS) in the maritime domain. Maintaining a proactive and comprehensive approach to cybersecurity becomes essential as the industry evolves to ensure the integrity, resilience, and safety of maritime operations in the digital age.

In chapter eight, various organizations, agencies, and resources are introduced to guide and support maritime entities in developing and implementing cybersecurity plans. This chapter underscores the absence of a universal, one-size-fits-all approach to cyber planning in the maritime sector. It acknowledges that while ports, ships, shipping lines, manufacturers, and other stakeholders in the MTS share commonalities, their cybersecurity requirements and defense strategies differ. The focus is on addressing the unique needs and challenges of each entity within the diverse landscape of the maritime industry.

In conclusion, this book highlights the intricacies of the maritime transportation system and the myriad of attack vectors within the cyber landscape, further complicated by the sector's fragmented adoption of new technologies. It advocates for maritime organizations to embrace an all-hazards approach, emphasizing the importance of foundational cybersecurity practices and constant vigilance against all threats. While recognizing the sophistication of adversaries, the book stresses the necessity of maintaining high standards of care, adhering to industry best practices, and continuously investing in the education and training of personnel. These

measures are essential in reinforcing cybersecurity as a fundamental aspect of the maritime community's safety culture.

Reviewed by Ayesha Abrar, MPhil scholar at the Strategic Studies Department of National Defence University (NDU), Islamabad.