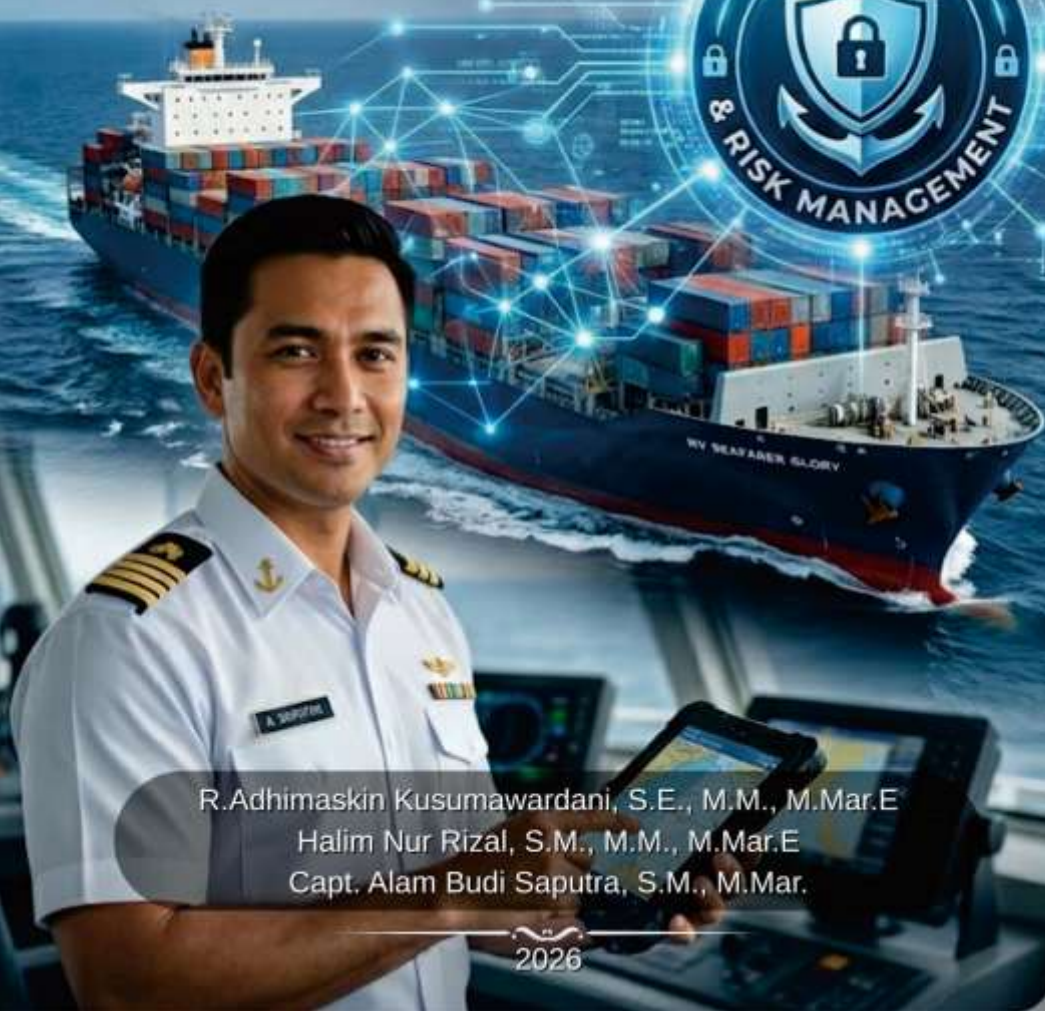




CYBER SECURITY for SEAFARER

Cyber Awareness, Safety and
Risk Management Onboard Ships



R.Adhimaskin Kusumawardani, S.E., M.M., M.Mar.E
Halim Nur Rizal, S.M., M.M., M.Mar.E
Capt. Alam Budi Saputra, S.M., M.Mar.

CYBER SECURITY FOR SEAFARER

Penulis:

R.Adhimaskin Kusumawardani, S.E., M.M., M.Mar.E

Halim Nur Rizal, S.M., M.M., M.Mar.E

Capt. Alam Budi Saputra, S.M., M.Mar



UU No. 28 Tahun 2014 tentang Hak Cipta

Fungsi dan Sifat Hak Cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Keteistuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

- i. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
- ii. penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
- iii. penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan fonogram yang telah dilakukan pengumuman sebagai bahan ajar; dan
- iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000,00 (seratus juta rupiah).
2. Setiap orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

CYBER SECURITY FOR SEAFARER

R.Adhimaskin Kusumawardani, S.E., M.M., M.Mar.E

Halim Nur Rizal, S.M., M.M., M.Mar.E

Capt. Alam Budi Saputra, S.M., M.Mar

TATA LETAK:

Sari

DESAIN SAMPUL:

Adhar

SUMBER:

www.tdjpublisher.com

ISBN:

978-634-279-082-3

CETAKAN PERTAMA:

April 2026

UKURAN:

vi + 69 Hal; 15,5 cm x 23 cm

Hak Cipta dilindungi Undang-Undang.

Dilarang menggandakan atau memperbanyak sebagian atau seluruh isi buku ini dalam bentuk apa pun tanpa izin tertulis dari penerbit dan penulis.

ANGGOTA IKAPI: 006/NTT/2022

TANGGUH DENARA JAYA PUBLISHER

Jl. Timor Raya No. 130 B, Kota Kupang, NTT

E-mail: tdj.denarapublisher@gmail.com

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya buku *Maritime Cyber Security for Seafarer* ini dapat disusun dan diselesaikan. Buku ini disusun sebagai respons atas meningkatnya penggunaan sistem digital di atas kapal serta berkembangnya ancaman siber yang berpotensi memengaruhi keselamatan pelayaran, perlindungan lingkungan laut, dan keberlangsungan operasi kapal.

Dalam era pelayaran modern, awak kapal tidak hanya dituntut memiliki kompetensi teknis navigasi dan mesin, tetapi juga pemahaman yang memadai mengenai keamanan siber. Gangguan terhadap sistem navigasi, komunikasi, mesin, maupun administrasi kapal akibat serangan siber dapat berdampak langsung pada keselamatan manusia, kapal, dan muatan. Oleh karena itu, kesadaran dan kesiapsiagaan awak kapal terhadap risiko siber menjadi kebutuhan yang tidak terpisahkan dari sistem keselamatan kapal.

Buku ini dirancang sebagai buku ajar yang praktis dan aplikatif bagi seafarer. Materi disusun secara sistematis, mulai dari pengenalan sistem digital di atas kapal, jenis ancaman siber, peran awak kapal, prosedur pengamanan, tanggap darurat insiden siber, hingga integrasi keamanan siber ke dalam *Safety Management System (SMS)*. Selain itu, buku ini juga dilengkapi dengan studi kasus, simulasi, serta pembelajaran operasional yang diharapkan dapat membantu awak kapal memahami penerapan *cyber security* dalam situasi nyata.

Penulis menyadari bahwa buku ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang bersifat membangun sangat diharapkan untuk penyempurnaan pada edisi selanjutnya. Semoga buku ini dapat memberikan manfaat bagi seafarer, instruktur pelatihan, serta seluruh pihak yang terlibat

dalam upaya peningkatan keselamatan dan keamanan pelayaran di era digital.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dan referensi dalam penyusunan buku ini. Semoga buku ini dapat menjadi kontribusi nyata dalam membangun budaya keselamatan siber di dunia pelayaran.

Jakarta, April 2026

Penulis

DAFTAR ISI

KATA PENGANTAR.....	i
DAFTAR ISI	iii
PENDAHULUAN UMUM.....	v
BAB I PENDAHULUAN	1
1.1. Cyber Security dalam Operasi Kapal	1
1.2. Ancaman Siber terhadap Keselamatan Pelayaran	3
1.3. Tujuan Buku bagi Awak Kapal.....	5
BAB II SISTEM DIGITAL DI ATAS KAPAL	7
2.1. Bridge System & Navigation	7
2.2. Engine & Machinery Control System	9
2.3. Communication & Satellite System	11
2.4. Crew Welfare & Admin System	13
BAB III ANCAMAN SIBER DI KAPAL.....	15
3.1. Cyber Attack pada Navigasi.....	15
3.2. Gangguan Sistem Mesin & OT	17
3.3. Social Engineering terhadap Awak Kapal	19
3.4. Risiko USB, Laptop & Perangkat Pribadi.....	20
BAB IV HUMAN FACTOR & CYBER AWARENESS	23
4.1. Peran Awak Kapal dalam Cyber Security	23
4.2. Kesalahan Umum Crew	25
4.3. Cyber Hygiene di Atas Kapal.....	27
4.4. Budaya Keselamatan Siber.....	31
BAB V PROSEDUR KEAMANAN SIBER DI KAPAL	34
5.1. Akses Sistem & Password Management.....	34

5.2.	Penggunaan Media Eksternal.....	36
5.3.	Update & Patch Management	38
5.4.	Segregasi IT & OT	41
BAB VI TANGGAP DARURAT INSIDEN SIBER.....		44
6.1.	Identifikasi Insiden Siber	44
6.2.	Tindakan Awal Awak Kapal	46
6.3.	Pelaporan ke Company & CSO	48
6.4.	Perlindungan Keselamatan Kapal	50
BAB VII INTEGRASI CYBER SECURITY KE ISM Code ...		52
7.1.	Cyber Risk dalam SMS.....	52
7.2.	Checklist Cyber Security Kapal.....	54
7.3.	Drill & Training Cyber Incident.....	57
BAB VIII STUDI KASUS & SIMULASI.....		60
8.1.	Kasus Nyata Serangan Siber Kapal	60
8.2.	Simulasi Insiden untuk Crew	62
8.3.	Pembelajaran Operasional.....	64
BAB IX PENUTUP		66
9.1.	Kesimpulan	66
9.2.	Pesan Keselamatan untuk Seafarer	67
DAFTAR PUSTAKA.....		68