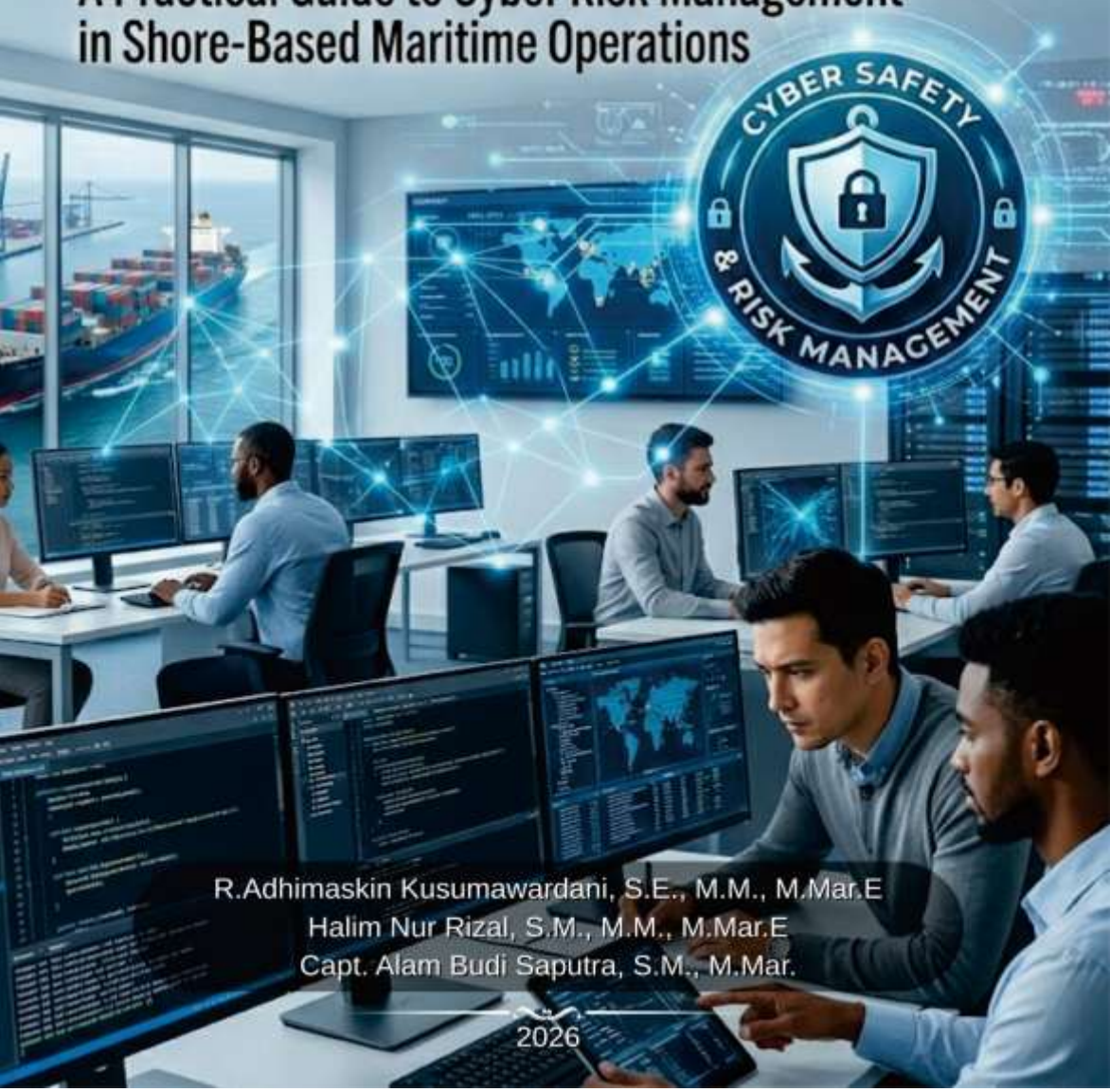




MARITIME CYBER SECURITY for OFFICE

A Practical Guide to Cyber Risk Management
in Shore-Based Maritime Operations



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.

MARITIME CYBER SECURITY FOR OFFICE

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

Keterbatasan 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).

Maritime Cyber Securty for Office

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:

978-634-279-083-0

CETAKAN PERTAMA:

April 2026

UKURAN:

vi + 89 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

Perkembangan teknologi digital telah membawa perubahan fundamental dalam industri maritim global. Digitalisasi sistem operasional, integrasi *ship–shore interface*, serta pemanfaatan *cloud computing* dan layanan pihak ketiga telah meningkatkan efisiensi dan transparansi operasi pelayaran. Namun, di sisi lain, transformasi ini juga menghadirkan tantangan baru berupa meningkatnya risiko siber (*cyber risk*) yang berpotensi memengaruhi keselamatan, keamanan, dan keberlangsungan operasi maritim.

Buku *Maritime Cyber Security for Office* disusun sebagai respons terhadap kebutuhan akan pemahaman yang komprehensif dan terstruktur mengenai keamanan siber maritim dari perspektif organisasi darat (*shore-based organization*). Fokus utama buku ini adalah memberikan kerangka konseptual, regulatif, dan praktis bagi manajemen perusahaan pelayaran, staf operasional, serta pemangku kepentingan maritim dalam mengelola risiko siber secara sistematis dan selaras dengan standar internasional.

Pembahasan dalam buku ini mengacu pada *Guidelines on Maritime Cyber Risk Management* yang dikeluarkan oleh International Maritime Organization (IMO), termasuk integrasinya ke dalam *Safety Management System* sesuai *ISM Code* dan keterkaitannya dengan *ISPS Code*. Selain itu, buku ini juga mengelaborasi praktik terbaik industri, studi kasus insiden siber maritim, serta pendekatan manajemen risiko dan *business continuity* yang relevan dengan konteks operasional perusahaan pelayaran.

Penulis menyadari bahwa keamanan siber bukan semata-mata isu teknis, melainkan isu tata kelola (*governance*), kepemimpinan, dan budaya organisasi. Oleh karena itu, buku ini disusun dengan pendekatan akademik-aplikatif, agar dapat digunakan sebagai bahan ajar, modul pelatihan, maupun referensi praktis bagi organisasi maritim yang ingin membangun ketahanan siber (*cyber resilience*) secara berkelanjutan.

Akhir kata, penulis berharap buku ini dapat memberikan kontribusi nyata dalam meningkatkan kesadaran, pemahaman, dan kesiapan industri maritim Indonesia dan global dalam menghadapi tantangan keamanan siber di era digital. Segala kritik dan saran yang bersifat konstruktif sangat diharapkan demi penyempurnaan karya ini di masa mendatang.

Jakarta, April 2026

Penulis

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	iii
PENDAHULUAN UMUM	v
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Cyber Security Maritim.....	1
1.2. Digitalisasi & Risiko Siber di Industri Maritim	2
1.3. Tujuan dan Ruang Lingkup Modul	4
1.4. Dasar Regulasi.....	6
BAB II KONSEP DASAR CYBER SECURITY MARITIM	9
2.1. Pengertian <i>Cyber Security & Cyber Risk</i>	9
2.2. IT System vs OT System di Maritim	10
2.3. Ancaman Siber pada Kantor Pelayaran	13
2.4. Cyber Risk dalam Perspektif Manajemen	15
BAB III KERANGKA REGULASI & STANDAR INTERNASIONAL	18
3.1. IMO Guidelines on Maritime Cyber Risk Management	18
3.2. Integrasi Cyber Risk ke ISM Code	20
3.3. Kaitan dengan ISPS Code & Port Security.....	22
3.4. Peran Administrasi & Flag State.....	24
BAB IV SISTEM & INFRASTRUKTUR KANTOR PELAYARAN.....	26
4.1. Sistem Informasi Perusahaan Pelayaran	26
4.2. Ship–Shore Interface.....	28
4.3. Data Management & Cloud Risk	30
4.4. Vendor & Third-Party Risk	33
BAB V ANCAMAN & SERANGAN SIBER	36
5.1. Malware, Ransomware, Phishing	36
5.2. Insider Threat	39
5.3. Supply Chain Attack	41
5.4. Studi Kasus Insiden Siber Maritim	43

BAB VI CYBER RISK MANAGEMENT	47
6.1. Identifikasi Risiko Siber.....	47
6.2. Penilaian & Evaluasi Risiko	49
6.3. Pengendalian & Mitigasi Risiko	51
6.4. Cyber Risk Register	53
BAB VII TATA KELOLA & ORGANISASI CYBER SECURITY	57
7.1. Peran Top Management.....	57
7.2. Cyber Security Policy	58
7.3. SOP & Awareness Program.....	61
7.4. Audit & Continuous Improvement	63
BAB VIII INCIDENT RESPONSE & BUSINESS CONTINUITY	66
8.1. Deteksi & Pelaporan Insiden.....	66
8.2. Penanganan Insiden Siber	68
8.3. Disaster Recovery Plan	70
8.4. Lessons Learned.....	72
BAB IX PENUTUP	75
9.1. Kesimpulan.....	75
9.2. Rekomendasi Implementasi	76
DAFTAR PUSTAKA.....	78

PENDAHULUAN UMUM

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital secara masif di sektor maritim, khususnya pada organisasi pelayaran, perusahaan pengelola kapal, dan institusi pendukung operasional maritim. Pemanfaatan *information technology* (IT), *operational technology* (OT), sistem berbasis jaringan, serta integrasi data *ship–shore* telah meningkatkan efisiensi, akurasi pengambilan keputusan, dan daya saing industri pelayaran secara global. Namun demikian, digitalisasi tersebut secara simultan juga memperluas *attack surface* dan meningkatkan eksposur organisasi maritim terhadap berbagai risiko siber (*cyber risk*).

Dalam konteks industri pelayaran, ancaman siber tidak lagi terbatas pada gangguan sistem informasi administratif, tetapi berpotensi menimbulkan dampak sistemik terhadap keselamatan pelayaran, keamanan kapal, kontinuitas bisnis, perlindungan data strategis, serta reputasi perusahaan. Serangan *malware*, *ransomware*, *phishing*, dan *supply chain attack* yang menargetkan kantor pelayaran dapat berimplikasi langsung pada operasi kapal, pengelolaan armada, sistem logistik, hingga kepatuhan terhadap regulasi internasional. Oleh karena itu, *cyber security* tidak dapat dipandang semata-mata sebagai isu teknis, melainkan sebagai isu manajerial, strategis, dan tata kelola organisasi.

Sejalan dengan dinamika tersebut, komunitas maritim internasional melalui *International Maritime Organization* (IMO) telah menegaskan pentingnya pengelolaan risiko siber melalui berbagai instrumen regulasi dan pedoman, antara lain *Guidelines on Maritime Cyber Risk Management* serta integrasi manajemen risiko siber ke dalam *Safety Management System* (SMS) sebagaimana ditegaskan dalam Resolusi MSC.428(98). Regulasi ini menempatkan *cyber risk management* sebagai bagian integral dari sistem keselamatan dan keamanan pelayaran, yang harus diterapkan

secara sistematis oleh perusahaan pelayaran, baik di tingkat kapal maupun kantor (*shore-based organization*).

Buku “Maritime Cyber Security for Office” disusun sebagai referensi akademik dan praktis yang berfokus pada pengelolaan keamanan siber di lingkungan kantor pelayaran dan organisasi pendukung maritim. Buku ini menekankan pendekatan *risk-based*, *management-driven*, dan selaras dengan kerangka regulasi internasional, dengan tujuan memberikan pemahaman komprehensif mengenai konsep, ancaman, tata kelola, serta strategi mitigasi risiko siber yang relevan bagi level manajemen, profesional maritim, dan pemangku kepentingan terkait.

Dengan pendekatan yang sistematis, analitis, dan berbasis regulasi, buku ini diharapkan dapat menjadi landasan konseptual dan operasional dalam membangun ketahanan siber (*cyber resilience*) organisasi maritim, serta mendukung terwujudnya operasi pelayaran yang aman, andal, dan berkelanjutan di era digital.