AN A.S. PRATT PUBLICATION
JANUARY 2017
VOL. 3 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 1 | JANUARY 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [297] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

IMO Interim Guidelines: Recent Developments in Maritime Cyber Risk Management

By Kate B. Belmont*

The author of this article discusses the International Maritime Organization Interim Guidelines on Maritime Cyber Risk Management, which is a call to action for the maritime industry.

Cyber risk management continues to be one of the most significant challenges currently facing the maritime industry. With an overreliance on information technology ("IT") and operational technology ("OT"), the shipping industry is vulnerable to cyber risks, cyber threats, and cyber attacks that could result in significant damages and loss, including loss of business and damage to reputation and property. While the maritime industry has yet to be regulated, various stakeholders have recognized the need for the industry to address cyber risk. As the U.S. Coast Guard continues to assess and evaluate cyber risk throughout the marine transportation system, the International Maritime Organization ("IMO") and various industry organizations have issued guidelines on cyber risk management this past year. Most notably, the IMO approved Interim Guidelines on Maritime Cyber Risk Management ("IMO Interim Guidelines").

THE SIGNIFICANCE OF THE IMO INTERIM GUIDELINES

The IMO Interim Guidelines are high-level recommendations for maritime cyber risk management, and are intended for all organizations in the shipping industry. This is a significant development as "The Guidelines on Cyber Safety and Security Onboard Ships" ("Industry Guidelines for Onboard Ships"), which was produced by BIMCO, CLIA, ICS, INTERCARGO, and INTERANKO and released in January of 2016, is limited in its recommendations to cyber risk management for onboard ship operations. In contrast, the IMO Interim Guidelines provide recommendations for safety and secure management practices for all stakeholders in the shipping industry. How does the release of these guidelines affect the maritime industry? While no regulations have been established yet, both sets of guidelines have created a greater level of care and can now be considered best practices for owners and operators, and should be carefully considered and incorporated into current safety and security risk management processes.

* Kate B. Belmont is an associate at Blank Rome LLP concentrating her practice in the areas of admiralty and maritime law, commercial litigation, and arbitration. She may be contacted at kbelmont@blankrome.com.

ADDRESSING CYBER RISK MANAGEMENT

In addressing cyber risk management, the IMO Interim Guidelines outline various systems used throughout the marine environment that are susceptible to cyber risk. Vulnerable systems include:

- bridge systems;
- cargo handling and management systems;
- passenger servicing and management systems;
- access control systems; and
- communication systems.

Accessing or interconnecting these systems leads to cyber risk, and as cyber technologies have become essential to the maritime industry, these systems must be protected. Significantly, the IMO Interim Guidelines make the distinction between IT and OT systems, which is critical in the greater understanding of cyber risk. IT systems focus on the use of data as information and are commonly identified as transaction systems, including business systems and information systems. OT systems focus more on the use of data to control or monitor physical processes or equipment. As the maritime industry is reliant on both IT and OT systems, it is important to understand that cyber risk extends to all systems that are reliant on information communication technology—for example, systems operated by finance and administrative departments and those operated by engineers, technicians, and crew.

The IMO Interim Guidelines state that vulnerabilities in these systems can be exploited intentionally or unintentionally. The threats facing these systems range from intentional, malicious actions, including hacking or introduction of malware, to unintentional consequences of poor cyber risk management, including outdated software, ineffective firewalls, the absence of network segregation, and procedural lapses. While the IMO Interim Guidelines do not address every possible cyber threat and vulnerability, these guidelines make clear that effective cyber risk management should consider all kinds of threats. The IMO also correctly notes that these technologies and threats are constantly changing, therefore effective cyber risk management must be holistic and flexible and evolve as a natural extension of existing safety and security management practices.

The IMO Interim Guidelines address the elements of effective cyber risk management, which is defined as "the process of identifying, analyzing, assessing, and communication cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level considering costs and benefits of actions taken to stakeholders." Both the IMO Interim Guidelines and the Industry Guidelines for Onboard Ships state that effective risk management should start at the senior management level. To best achieve effective cyber risk management, a culture of cyber risk awareness must be

incorporated into all levels of an organization. Cyber risk policies and procedures can be unique to each organization and must be constantly evaluated and evolving.

A CALL TO ACTION FOR THE MARITIME INDUSTRY

Owners and operators must take heed of the Interim Guidelines on Maritime Cyber Risk Management. Although "recommendatory," along with the Guidelines on Cyber Safety and Security Onboard Ships, a new standard of care and best practices have been established in the maritime industry. Owners and operators will be held to a higher standard when dealing with loss and damages resulting from a cyber attack or breach. Cyber threats, vulnerabilities, and loss have plagued the maritime industry for years, but effective cyber risk management has only recently become a priority. That said, owners and operators can no longer claim ignorance to dangers posed by cyber threats and must take the appropriate steps to mitigate cyber risk and avoid potential liability for any loss or damages resulting from a cyber breach or attack.

Ports continue to be targets for cyber attacks from malicious actors, mainland IT systems at major shipping companies continue to be besieged with malware and spear-phishing campaigns, and onboard ship systems continue to be vulnerable to intentional and unintentional cyber threats. With its overreliance on IT and OT systems, its reliance on outdated software, and its failure to develop current and effective cybersecurity practices, the maritime industry is faced with the unique challenge of mitigating cyber risk on many different levels. While the IMO Interim Guidelines are not mandatory, they serve as a baseline for better understanding and mitigating cyber risk, and should be referenced in developing sound cyber risk management policies and procedures. Failure to actively engage in cyber risk management will result in increased liability for owners and operators.

For additional guidance on the implementation of cyber risk management procedures and practices, the IMO also recommends referring to the Guidelines on Cyber Safety and Security Onboard Ships; ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems–Requirements; and the United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Security (the NIST Framework).