AN A.S. PRATT PUBLICATION
JULY-AUGUST 2023
VOL. 9 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 6** **July - August 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home/
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) 487-3385

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 [82] (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

(2023–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, 631.291.5541. 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.

Maritime Ransomware

By Vanessa C. DiDomenico, Sharon R. Klein and Karen H. Shin*

In this article, the authors explain that shipowners and operators should not only develop cybersecurity plans, but should also have counsel throughout the incident response and recovery.

Cybersecurity concerns are certainly on the radar for shipowners and operators. Cybersecurity breaches can penetrate systems aboard and ashore and can jeopardize safety and adversely impact maritime operations, as well as disrupt the downstream distribution of the goods on board. In that light, it is imperative that shipowners and operators install tough mitigation, detection, and response plans.

As ships undergo digitalization and autonomous system upgrades, cyberattacks and ransomware attempts become more prevalent. Ransomware is defined as a type of malicious software designed to block access to a computer system until the attacked party pays a sum of money. Cybercriminals monetize their operations by extorting their victims and can further sell extracted data. Cyberattackers typically seek the highest payout possible and target companies and industries, including the maritime sector, that rely on time-sensitive data to function. Such attacks can have devastating contemporaneous consequences on multiple players.

RANSOMWARE ATTACKS

In the 2017 NotPetya malware incident, attackers encrypted Maersk systems and demanded payment. "Without access to data held on its destroyed computer system, Maersk literally didn't know what was in its containers. On-the-ground-staff had to check manually, with time sensitive medicines a particular supply chain concern."[1] The attackers shut down systems in seven minutes, but the response and industry's realization that protections were needed lasted much longer. "The key lesson Maersk learned from battling the NotPetya attack: protection is important – but it's equally as important to ensure your recovery process is strong."[2]

---

* The authors, attorneys with Blank Rome LLP, may be contacted at vanessa.didomenico@blankrome.com, sharon.klein@blankrome.com and karen.shin@blankrome.com, respectively.

[1] Adam Bannister, "When the screens went black: How NotPetya taught Maersk to rely on resilience—not luck—to mitigate future cyber-attacks" (July 6, 2021), available at: portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks.

[2] Danny Palmer, "Ransomware: The key lesson Maersk learned from battling the NotPetya attack" (April 29, 2019), available at: zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack.

Notably, on May 6, 2021, the Colonial Pipeline incident made headlines when that company paid $4.4 million in ransom after the major supplier of oil was unable to access or control its IT systems that affected 45 percent of fuel supplied to the East Coast.

Further, in 2021, Transnet, the South African port operator, declared force majeure after a ransomware attack halted its IT systems and disrupted container operations at a number of its ports, including Durban, Cape Town, and Port Elizabeth.

In February 2022, ports in Germany, Belgium, and the Netherlands were all affected by a ransomware attack that delayed oil terminal operations and crippled port systems.

A ferry operator in Massachusetts, the Steamship Authority, was also the target of a debilitating ransomware attack that reverberated across its operations, which provide the transportation lifeline to the islands of Nantucket and Martha's Vineyard, crashing the company's website, halting vehicle reservations, and disabling internal communication systems.

Most recently, on January 7, 2023, DNV's ShipManager servers fell victim to a ransomware cyberattack. About 70 customers, operating around 1,000 vessels, were affected.[3]

There are numerous other examples of ransomware attacks; however, not all instances are publicly disclosed. In some cases, ransomware attacks go unreported, and companies opt to pay money to the attackers without seeking government assistance. The U.S. Treasury Department estimated that $1.2 billion was paid in 2021 to ransomware actors. Unfortunately, in over 35 percent of the cases where money was paid, the attackers did not restore the data or refrain from returning in a future attack. The Office of Foreign Assets Control (OFAC) warned that paying ransom may constitute a violation of economic sanctions laws, be a threat to national security, and encourage future attacks. The U.S. government is further turning its focus to requiring the reporting of ransomware attacks. In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act. The act requires companies that power the country's critical infrastructure to report "substantial" cyber incidents to CISA within seventy-two (72) hours and to report payments made for ransomware attacks within 24 hours. Incidents can also be voluntarily reported[4] to the Cybersecurity & Infrastructure Security Agency (CISA). This U.S. agency works with partners to defend against cyber threats and collaborates with partners to build a more secure and resilient infrastructure.

[3] DNV, "Cyber-attack on ShipManager servers – update" (January 23, 2023), available at: dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931.

[4] https://www.cisa.gov/forms/report.

In July 2021, President Biden signed a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.[5] This memorandum required the Cybersecurity and Infrastructure Security Agency, in coordination with the National Institute of Standards and Technology and the interagency community, to develop baseline cybersecurity performance goals[6] that are consistent across all critical infrastructure sectors. These goals include recommended actions for account and device security, data security, governance and training, vulnerability management, supply chain / third parties, and response and recovery. The government has also launched StopRansomware.gov[7] to provide resources to tackle ransomware more effectively.

IMPORTANCE OF CYBERSECURITY

Port agencies are further highlighting the importance of cybersecurity. In January 2022, the Port of Los Angeles debuted[8] its Cyber Resilience Center, a cyber-defense solution created to improve the cybersecurity readiness of the Port by enabling participating stakeholders to automatically share cyber-threat indicators and potential defensive measures with each other. Shipowners and operators must prepare, detect, and respond to cyber incidents. According to data from the IBM Security Cost of a Data Breach Report 2022 analysis compiled by the Ponemon Institute, the average cost of a ransomware attack, not including the ransom itself, is $4.54 million. Additionally, the report found that the average savings associated with an incident response team and regularly tested incident response plans is $2.66 million.

CONCLUSION

It is important to not only develop cybersecurity plans, but to have counsel throughout the incident response and recovery, including but not limited to assistance in implementing and maintaining requisite data security safeguards such as written information security programs to comply with data security laws, and advising on data breach notifications to affected individuals and the requisite governmental/regulatory authority. Companies can lower cyber risks by conducting annual risk assessments and awareness training, implementing strategic IT investments, analyzing vendor management security commitments, and evaluating insurance coverage.

---

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

[6] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

[7] https://www.cisa.gov/stopransomware.

[8] https://www.cisa.gov/stopransomware.

If a cyber incident does occur, the first 24 hours are critical to investigating the breach, including identifying the nature of the breach, the categories of information compromised, how many individuals have been affected, the cause of the compromise, and the likely consequences of the breach and the risks to affected individuals, and to immediately begin remediation. The company's incident response plan should be followed, and relevant stakeholders within and outside the company should be notified (e.g., general counsel, company board, internal communications department, insurance brokers, government regulators, and affected individuals). Experienced counsel can also assist with notices that are regulatorily and contractually required, and help draft security, privacy, and indemnification clauses in vendor contracts, and in acquisitions to ensure that all parties partner in mitigating cyber security risk. In this realm, advance planning and proper execution of those plans is the key to weathering a cybersecurity storm.