AN A.S. PRATT PUBLICATION
OCTOBER 2021
VOL. 7 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: QUESTIONS AND ANSWERS
Victoria Prussen Spears

FIVE THINGS YOU SHOULD EXPECT TO BE ASKED AFTER A CYBER SECURITY INCIDENT
Keily Blair, James Lloyd, Aravind Swaminathan, and Laura Nonninger

FTC SETTLES COPPA ACTION AGAINST "COLORING BOOK FOR ADULTS"
Tracy Shapiro and Libby J. Weingarten

SECOND CIRCUIT ARTICULATES INJURY STANDARD IN DATA BREACH SUITS
Rahul Mukhi and JD Colavecchio

SUED FOR A DATA BREACH OUT OF STATE? DON'T FORGET A PERSONAL JURISDICTION DEFENSE
Timothy J. St. George, Ronald I. Raether, and David N. Anthony

FIFTH CIRCUIT LATEST TO CRY TAINT ON DOJ TAINT TEAM
Elliot S. Rosenwald, Marcus A. Asner, and Alexis Gannaway

RECENT CYBERSECURITY AND RANSOMWARE GUIDANCE THAT EVERY BUSINESS SHOULD BE REVIEWING
Elizabeth F. Hodge and Christy S. Hawkins

FRENCH COURT PROVIDES GUIDANCE ON DATA TRANSFER SAFEGUARDS AND SUFFICIENT PROTECTIONS AGAINST ACCESS REQUESTS FROM U.S. AUTHORITIES
Ricky C. Benjamin and Christy S. Hawkins

PRC DATA SECURITY LAW: WHAT YOU NEED TO KNOW
Clarice Yue, Michelle Chan, Sharon Zhang, and Tiantian Ke

CHINA PUBLISHES NEW DRAFT REGULATIONS ON DATA SECURITY MANAGEMENT OF AUTOMOBILE OPERATORS TO PROTECT PRIVACY
Jenny (Jia) Sheng, Chunbin Xu, and Esther Tao

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 8** **October 2021**

Editor's Note: Questions and Answers
Victoria Prussen Spears 251

Five Things You Should Expect to Be Asked After a Cyber Security Incident
Keily Blair, James Lloyd, Aravind Swaminathan, and Laura Nonninger 254

FTC Settles COPPA Action Against "Coloring Book for Adults"
Tracy Shapiro and Libby J. Weingarten 259

Second Circuit Articulates Injury Standard in Data Breach Suits
Rahul Mukhi and JD Colavecchio 264

Sued for a Data Breach Out of State? Don't Forget a Personal Jurisdiction Defense
Timothy J. St. George, Ronald I. Raether, and David N. Anthony 267

Fifth Circuit Latest to Cry Taint on DOJ Taint Team
Elliot S. Rosenwald, Marcus A. Asner, and Alexis Gannaway 271

Recent Cybersecurity and Ransomware Guidance That Every Business Should Be Reviewing
Elizabeth F. Hodge and Christy S. Hawkins 274

French Court Provides Guidance on Data Transfer Safeguards and Sufficient Protections Against Access Requests from U.S. Authorities
Ricky C. Benjamin and Christy S. Hawkins 279

PRC Data Security Law: What You Need to Know
Clarice Yue, Michelle Chan, Sharon Zhang, and Tiantian Ke 283

China Publishes New Draft Regulations on Data Security Management of Automobile Operators to Protect Privacy
Jenny (Jia) Sheng, Chunbin Xu, and Esther Tao 287

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) 487-3385
Fax Number ..... (800) 828-8341
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 ..... (937) 247-0293

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [251] (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

(2021–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.

Recent Cybersecurity and Ransomware Guidance That Every Business Should Be Reviewing

By Elizabeth F. Hodge and Christy S. Hawkins*

This article summarizes some of the recent guidance from the White House and the Cybersecurity and Infrastructure Security Agency to help businesses protect themselves against ransomware.

In response to the ever-increasing number of ransomware attacks, including several recent high-profile and high impact incidents, the Biden administration has recently issued several alerts and guidance documents regarding steps businesses can take to prevent disruption of their operations due to ransomware and other cyberattacks. These documents are required reading for organizations in all sectors, though businesses that operate or control critical infrastructure assets should pay especially close attention. While the administration is taking steps to prevent and respond to cyberattacks, the recent guidance makes clear that the administration expects the private sector to do its part to limit the impact of ransomware attacks.

This article summarizes some of the recent guidance from the White House and the Cybersecurity and Infrastructure Security Agency ("CISA") to help businesses protect themselves against ransomware.

EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

On May 12, 2021, President Biden issued an Executive Order on Improving the Nation's Cybersecurity (the "Executive Order").[1] The Executive Order outlines a number of steps that the federal government will take to modernize the government's IT infrastructure, including:

- Improving supply chain security by providing guidelines for how federal agencies must evaluate the software products and services they purchase;
- Deploying multi-factor authentication, endpoint detection and response, and encryption;

* Elizabeth F. Hodge is a partner at Akerman LLP concentrating her practice on compliance and regulatory issues affecting healthcare providers and payers and employer-sponsored health plans. Christy S. Hawkins (CIPP/US, CIPP/E, CIPM, FIP, PLS) is an associate at the firm focusing her practice on privacy, cybersecurity, and incident response. The authors may be contacted at elizabeth.hodge@akerman.com and christy.hawkins@akerman.com.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

- Adopting "zero trust" architecture and using more secure cloud services;
- Establishing a Cyber Incident Review Board to investigate cyber incidents and make recommendations;
- Removing barriers that prevent federal agencies and vendors from sharing threat intelligence data; and
- Creating standards to minimize the damage from ransomware incidents.

While the Executive Order is directed to action by the federal government, organizations that contract with federal agencies may also feel the impact of the Executive Order if the government insists on amending agreements to require more robust information security protections.

WHITE HOUSE MEMORANDUM TO CORPORATE EXECUTIVES AND BUSINESS LEADERS

Following the Executive Order, on June 2, 2021, the White House issued a memorandum to corporate executives and business leaders titled "What We Urge You To Do To Protect Against The Threat of Ransomware" ("White House Memo").[2]

Specifically, the White House Memo encourages organizations to view ransomware not simply as a data theft risk, but as a risk to their core business operations. As such, business executives should "immediately convene their leadership teams to discuss the ransomware threat" and review their organization's security posture and business continuity plans to ensure they have the ability to continue or quickly restore operations. The memo also urges businesses to promptly undertake the following "U.S. Government's recommended best practices" to decrease their cyber risk:

- *Implement the following best practices from the Executive Order*:
    - Use of multifactor authentication since passwords are routinely compromised;
    - Deploying endpoint detection and response to identify malicious activity on a network and block it;
    - Encryption for data at rest and in transit to render such data unusable if it is stolen; and
    - Creating an empowered security team to patch systems rapidly and incorporate threat information into the company's defenses.

[2] https://image.connect.hhs.gov/lib/fe3915707564047b761078/m/1/8eeab615-15a3-4bc8-8054-81bc23a181a4.pdf.

- *Back up data, system images, and configurations, regularly test them, and keep backups offline.* Since many ransomware variants try to locate and either encrypt or delete accessible backups, it is imperative to keep current backups offline so the organization is able to restore its systems in the event of an attack. Also, organizations need to confirm that their backup systems actually work, preferably before a ransomware attack.

- *Update and patch systems promptly.* Software system patches are only effective if companies promptly install them. Organizations can ensure they are current in several ways, including using a centralized patch management system or a risk-based assessment strategy to support the patch management program.

- *Test the incident response plan.* As noted in the White House Memo, testing is the best way to expose gaps in an incident response plan. Testing should target the plan and the team itself, so that team members are not seeing the incident response plan for the first time when they are tasked with responding to a critical incident.

- *Check the security team's work.* Companies should engage third party penetration testers to verify the security of systems and the ability to respond to a sophisticated attack.

- *Segment networks.* Because cyber criminals are shifting from stealing data to disrupting operations, it is critical that companies separate their corporate business functions and manufacturing and/or production operations and limit internet access to operational networks. Also, companies should identify links between these networks and develop workarounds or manual controls to ensure that mission critical system networks can be segregated and continue operating if the corporate network is compromised.

All of the recommended best practices in the White House Memo are well known and considered to be fundamental to an effective information security program. As a result, an organization that does not implement one or more of the practices should be prepared to explain why it did not do so, especially if it experiences a cyberattack.

CISA OPERATIONAL TECHNOLOGY GUIDANCE

In response to recent ransomware attacks targeting critical infrastructure, on June 9, 2021, CISA issued a fact sheet on the rising ransomware threat to operational technology assets[3] and control systems ("OT Guidance"). Operational technology is

[3] https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf.

technology that controls and monitors industrial process assets and manufacturing/industrial equipment. The OT Guidance, like the White House Memo, emphasizes that "[a]ll organizations are at risk of being targeted by ransomware and have an urgent responsibility to protect against ransomware threats." CISA further warns that critical infrastructure owners and operators should "adopt a heightened state of awareness" and voluntarily implement recommendations in the OT Guidance, including:

- *Identify Critical Processes for Essential Services.* Companies should identify all critical processes that must continue without interruption to provide essential services.
- *Effective Workarounds and Manual Controls.* Organizations should have a plan to operate when facing an attack, including developing and testing workarounds and manual processes to ensure that the critical processes identified in the preceding step can be isolated and continue to operate without access to IT networks.
- *Network Segmentation.* Like the White House Memo, the OT Guidance recommends that organizations implement "robust" network segmentation between the information technology and operational technology networks. CISA notes that even if network segmentation is implemented, some critical operational processes may still depend on business functions performed by the IT network so organizations should promptly take steps to reduce such co-dependencies.
- *Strong Backup Procedures.* The OT Guidance encourages organizations to ensure that they have backup procedures in place and regularly test them. Backups should be isolated from network connections so they cannot be accessed by ransomware. Finally, CISA recommends performing a full restore of backups from scratch to test the backup procedure and to help map previously unknown dependencies.

CISA also emphasizes that it strongly discourages paying ransoms because that does not ensure that the company's data will be decrypted or that information systems and data will no longer be compromised, and it encourages further attacks.

HHS OCR CYBER ALERT

The U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") issued a cyber alert on June 9, 2021 encouraging healthcare organizations to review the White House Memo and take appropriate action. OCR also recommends that healthcare organizations review the recent CISA alert[4] about a critical VMware vulnerability that bad actors are attempting to exploit. OCR and CISA recommend that organizations promptly apply the available patch, even if out-of-cycle work is needed.

[4] https://www.vmware.com/security/advisories/VMSA-2021-0010.html.

NEXT STEPS

Collectively, the guidance documents specify what the federal government deems to be best practices to reduce the risk of a successful cyberattack. All companies should review the guidance documents and, if necessary, modify their data security practices and business continuity plans accordingly. Failure to take the basic steps outlined in the guidance documents could leave an organization the victim of a ransomware attack and having to defend its decision not to implement the White House and CISA recommendations.