AN A.S. PRATT PUBLICATION
OCTOBER 2020
VOL. 6 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 8** **OCTOBER 2020**

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*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (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

(2020–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, 646.539.8300. 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.

SEC's Examination Function Warns Its Registrants of Risks Associated with Dangerous Malware

By Peter I. Altman, Jason M. Daniel, Natasha G. Kohne, Michelle A. Reed, and Molly E. Whitman *

The authors discuss a recent "Risk Alert" issued by the Office of Compliance Inspections and Examinations highlighting several practices and procedures that it suggests may limit or prevent exposure to ransomware and other information security vulnerabilities.

For the past eight years, the Office of Compliance Inspections and Examinations ("OCIE") has included information security as a key element of its examinations. On July 10, 2020, OCIE released a "Risk Alert"[1] regarding the increasing frequency and sophistication of ransomware attacks targeting U.S. Securities and Exchange Commission ("SEC") registrants. The Risk Alert highlights best practices to protect against and respond to ransomware attacks.

RANSOMWARE THREAT INCREASES

Ransomware is a type of malware that infects a computer or network and encrypts the system's critical data until the victim pays a ransom to regain access. According to Beazley, one of the leading insurance carriers in the cybersecurity space, the use of ransomware increased by 25 percent in the first quarter of 2020.[2] OCIE notes in the Risk Alert that it has recently observed increased ransomware attacks targeting SEC registrants – i.e., broker-dealers, investment advisers and investment companies – as

* Peter I. Altman, a partner in the Los Angeles office of Akin Gump Strauss Hauer & Feld LLP, handles white collar and other enforcement and regulatory matters, securities class action litigation and internal investigations. Jason M. Daniel, a partner in the firm's Dallas office, focuses on securities trading and reporting advice, investment advisor compliance and registration, and securities advice in respect to mergers and acquisitions. Natasha G. Kohne, a partner in the firm's offices in San Francisco and Abu Dhabi, is co-head of the firm's cybersecurity, privacy and data protection practice. Michelle A. Reed, a partner in the firm's Dallas office, is co-head of the firm's cybersecurity, privacy and data protection practice. Molly E. Whitman, counsel in the firm's Los Angeles office, focuses on high-value, complex commercial litigation covering a broad range of substantive law. The authors may be contacted at paltman@akingump.com, jdaniel@akingump.com, nkohne@akingump.com, mreed@akingump.com, and mwhitman@akingump.com, respectively.

[1] Office of Compliance Inspections and Examinations, "Cybersecurity: Ransomware Alert," *available at* https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.

[2] https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html.

well as their third-party service providers. Specifically, the Risk Alert underscores the threat of Dridex malware, one of the most frequently used financial Trojans, being used specifically against the financial sector.[3]

This Risk Alert is the second alert OCIE has released concerning a particular malware variant. The first was issued in 2017 following the widespread WannaCry ransomware attack, which affected organizations in more than 100 countries. OCIE's particular warning about Dridex therefore is significant and must be heeded with great caution.

To combat ransomware like Dridex, OCIE encourages registrants to stay up-to-date with alerts released by other government agencies, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA")[4] and by the Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3").[5]

OCIE references CISA's June 30, 2020, update concerning Dridex, which explains in technical detail how threat actors often utilize email phishing campaigns to inject Dridex malware into network systems, particularly those in the financial services industry. CISA's update also includes a robust list of mitigation recommendations to combat Dridex tactics, techniques and procedures ("TTPs").

APPROACHES TO COMBAT RANSOMWARE

Some of the Risk Alert's recommendations that home in on ransomware include:

- *Access Rights and Controls*: The Risk Alert identifies numerous access control best practices to limit threat actors' ability to penetrate a system via ransomware. These best practices include restricting user access to the least privileged access possible at all times and removing that access immediately upon termination of employment or an engagement, implementing access protections such as strong password requirements and multifactor authentication, and controlling, monitoring and reviewing access approvals and privileges. OCIE also advises that registrants pay particular attention to the access rights of those with heightened privileges, such as administrators and service accounts.

- *Training and Awareness*: Email phishing is one of the key methods utilized by threat actors to deploy ransomware on a system. OCIE notes that financial

[3] Earlier this year, Dridex was included for the first time in Check Point Research's Global Threat Index as one of the top 10 most prevalent malware variants, and the third most prevalent during March 2020. *See* https://www.globenewswire.com/news-release/2020/04/09/2014156/0/en/March-2020-s-Most-Wanted-Malware-Dridex-Banking-Trojan-Ranks-On-Top-Malware-List-For-First-Time.html.

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

[5] https://www.ic3.gov/media/news/default.aspx.

institutions have increasingly been the targets of phishing campaigns, and encourages registrants to ensure their employees are sufficiently trained to identify potential phishing attacks and maintain heightened awareness of potential threats.

    - OCIE likely calls attention to phishing because there has been a significant increase in phishing attacks overall in 2020. Threat actors have largely used the coronavirus as a means to exploit unwary employees who may have more lax cybersecurity hygiene while working from home.

- *Incident Response and Resiliency*: The Risk Alert suggests that registrants should assess, test and periodically update their incident response plans ("IRPs") and make sure these plans address ransomware and other denial of service attacks. OCIE also encourages registered investment advisers ("RIAs") to ensure their IRPs include up-to-date procedures for complying with state and federal data breach notification and reporting laws and for notifying relevant parties, potentially including regulators, law enforcement and/or customers.

- *Data Loss Prevention*: OCIE highlights the need for operational resiliency, including the ability to access a secondary system to continue to operate critical applications if the primary system becomes unavailable due to a ransomware attack. The Risk Alert further emphasizes that registrants should implement vulnerability and patch management programs and keep them updated to prevent ransomware attacks.

    - OCIE emphasizes that registrants should back up their data and keep it geographically separated in case of an attack.

    - Notably, the Risk Alert also pinpoints perimeter security as a key tool in preventing ransomware attacks and advises that registrants employ best practices for use of Remote Desktop Protocol ("RDP") through an encrypted virtual private network ("VPN"). With a high percentage of the American workforce working from home, RDP presents a significant vulnerability for ransomware attacks.

    - Maintaining security capabilities to closely monitor all traffic through tools such as firewalls, intrusion detection systems, email security capabilities and web proxy systems with content filtering is also noted as a key practice to reduce ransomware threats.

CONCLUSION AND RECOMMENDATIONS

We recommend that registrants review the full list of identified best practices and procedures in the Risk Alert to avoid becoming the next victim of a ransomware threat and, further, that registrants share this alert with third parties that hold their data – especially administrators. With this alert, OCIE has signaled that how registrants control and respond to ransomware attacks will continue to be a focus of OCIE examinations.[6] OCIE referrals remain a common source for the opening of investigations by the Division of Enforcement, and registrants should thus pay close attention to the Risk Alert.

Registrants should also consider implementing the following measures, or reviewing existing measures for required updates, in addition to those OCIE identified:

1. Institute other best practices concerning RDP, including disabling RDP where it is not required, as RDP is one of the network features most vulnerable to a ransomware attack.

2. Establish procedures that make it simple for employees to immediately report suspicious emails and attachments. For example, implement a button within your email client to automatically forward a suspicious email to the designated IT response team, or create an easy-to-remember email account to which employees can send questionable communications.

3. Configure firewalls and other perimeter security capabilities to block known malicious IP addresses and other identified indicators of compromise ("IOCs").

4. Require multifactor authentication for all network access.

5. Contact outside counsel as soon as possible if data loss is known or suspected to ensure the greatest protection of investigation materials and conclusions under the attorney-client privilege.

6. Extend all policies and procedures to cover personal devices that are capable of accessing the organization's network.

[6] That this is the second OCIE alert issued in a short period of time advising registrants to keep a watchful eye out for deficiencies in their controls, policies, and procedures emphasizes that registrants must proactively monitor their compliance ahead of potential OCIE examinations.