# The Banking Law Journal

Established 1889

**An A.S. Pratt™ PUBLICATION** **MAY 2022**





LexisNexis

# THE BANKING LAW JOURNAL

**VOLUME 139** **NUMBER 5** **May 2022**



LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

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 Website . . . . . 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: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.



Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub.4815)

# *Editor-in-Chief, Editor & Board of Editors*

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten 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 inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. 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 THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

# CISA Issues Joint Cybersecurity Advisory on Ransomware Trends and Recommendations

***By Micaela McMurrough, Ashden Fein and Caleb Skeath****

*The authors of this article discuss a joint report coauthored by cybersecurity authorities in the United States, Australia and the United Kingdom. The report provides technical details regarding the observed behaviors and trends of ransomware actors, mitigation recommendations for network defenders to reduce their risk of compromise by ransomware, and step-by-step advice for responding to ransomware attacks.*

The Department of Homeland Security Cybersecurity & Infrastructure Security Agency ("CISA") has announced[1] the publication of a joint cybersecurity advisory[2] observing "an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally" during 2021. The report—which was coauthored by cybersecurity authorities in the United States (CISA, the Federal Bureau of Investigation, and the National Security Agency), Australia (the Australian Cyber Security Centre), and United Kingdom (the National Cyber Security Centre)—emphasizes that the continued evolution of ransomware tactics and techniques throughout the past year "demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally."

The joint report provides technical details regarding the observed behaviors and trends of ransomware actors, mitigation recommendations for network defenders to reduce their risk of compromise by ransomware, and step-by-step advice for responding to ransomware attacks.

---

* Micaela McMurrough is an attorney at Covington & Burling LLP representing clients in antitrust, patent, trade secrets, contract, and securities litigation, and other complex commercial litigation matters, and serves as co-chair of the firm's global and multi-disciplinary Internet of Things group. Ashden Fein is an attorney at the firm advising clients on cybersecurity and national security matters, including crisis management and incident response, risk management and governance, government and internal investigations, and regulatory compliance. Caleb Skeath is an attorney at the firm advising clients on a broad range of privacy and data security issues, including regulatory inquiries from the Federal Trade Commission, data breach notification obligations, compliance with consumer protection laws, and state and federal laws regarding educational and financial privacy.

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[2] https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf.

**RANSOMWARE TRENDS**

The report details a variety of behaviors and trends that cybersecurity authorities observed among cyber criminals over the past year.

- *Gaining Access to Networks*: The top three "initial infection vectors" for ransomware incidents in 2021 remained phishing emails, remote desktop protocols ("RDP") exploitation, and exploitation of software vulnerabilities.
- *Using Cyber Criminal Services-for-Hire*: The market for ransomware grew in sophistication in 2021, as ransomware threat actors not only made increased use of ransomware-as-a-service, but also "employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals." The advisory noted that this business model "often complicates attribution" of ransomware incidents to specific threat actor(s).
- *Sharing Victim Information*: Ransomware groups in Eurasia have shared victim information with each other, including selling access to victims' networks, which "diversif[ied] the threat to targeted organizations."
- *Shifting Away from "Big-Game" Hunting in the United States*: U.S. authorities observed that, over the course of 2021, some cybercriminals shifted their ransomware efforts from large organizations, including those that provide critical services, toward mid-sized victims after several high-profile incidents resulted in scrutiny and disruption from government authorities. Australian and UK authorities, however, observed that ransomware threat actors continued to target organizations of all sizes.
- *Diversifying Approaches to Extorting Money*: Ransomware threat actors increasingly used "triple extortion" methods as part of ransomware incidents by "threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim's internet access, and/or (3) inform the victim's partners, shareholders, or suppliers about the incident."
- *Increasing Their Impact*: Authorities observed that cybercriminals have increased the scale and disruptive nature of their attacks by targeting cloud infrastructures (including the cloud providers themselves), managed service providers ("MSPs"), industrial processes (including code designed to stop critical infrastructure or industrial processes), and the software supply chain, as well as by conducting attacks on holidays and weekends. The authorities authoring the alert assessed that "there will

be an increase in ransomware incidents where threat actors target MSPs to reach their clients."

## MITIGATION RECOMMENDATIONS

CISA's advisory identified five "immediate actions" that entities can "take now to protect against ransomware":

- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use RDP secure and monitor it.
- Make an offline backup of your data.
- Use multi-factor authentication ("MFA").

The report also advises that network defenders may "reduce the likelihood and impact of ransomware incident" by taking the following steps (some of which mirror CISA's immediate actions listed above):

- Keeping all operating systems and software up to date, including by prioritizing known exploited vulnerabilities and automating software security scanning and testing when possible;
- Securing and closely monitoring RDP or other potentially risky services, including external connections to third party vendors;
- Implementing a user training program and phishing exercises;
- Requiring multi-factor authentication for as many services as possible, "particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups;"
- Requiring all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords;
- If using Linux, using a Linux security module (such as SELinux, AppArmor, or SecComp) for defense in depth; and
- Protecting cloud storage by backing up to multiple locations, requiring MFA for access, and encrypting data in the cloud.

The report further recommends that network defenders may "limit an adversary's ability to learn an organization's enterprise environment and to move laterally" through the following steps:

- Segmenting networks;

- Implementing end-to-end encryption;
- Identifying, detecting, and investigating abnormal activity and potential traversal of the indicated ransomware with a network-monitoring tool;
- Documenting external remote connections;
- Implementing time-based access for privileged accounts;
- Enforcing principle of least privilege through authorization policies;
- Reducing credential exposure;
- Disabling unneeded command-line utilities; constraining scripting activities and permissions, and monitoring their usage;
- Maintaining offline (i.e., physically disconnected) backups of data, and regularly testing backup and restoration;
- Ensuring that all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure; and
- Collecting telemetry from cloud environments.

The advisory also recommended that critical infrastructure organizations with industrial control systems or operational technology ("OT") networks should review the joint CISA-FBI Cybersecurity Advisory DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks for more recommendations. CISA's mitigation recommendations align with steps that cyber insurance policyholders can take to manage ransomware risk as insurers have scaled back coverage in response to the increase in global ransomware attacks.

## RESPONDING TO RANSOMWARE ATTACKS

Finally, the report recommends that organizations take the following steps if involved in a ransomware attack:

- Follow the Ransomware Response Checklist on page 11 of the CISA-Multi-State Information Sharing and Analysis Center ("MS-ISAC") Joint Ransomware Guide;[3]
- Scan backup data with an antivirus program to check that it is free of malware, using an isolated, trusted system to avoid exposing backups to

[3] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

potential compromise;

- Report cybersecurity incidents to the appropriate authority; and
- Apply incident response best practices found in the joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity.[4]

The cybersecurity authorities in the United States, Australia and the United Kingdom "strongly discourage paying a ransom to criminal actors," because paying the ransom not only promotes the ransomware business model, but also does not guarantee recovery of the victim's files. In fact, the National Cyber and Security Centre has urged UK regulators to consider prohibiting insurance coverage for ransomware payments as a means of deterring ransomware attacks.

## RESOURCES

The joint cybersecurity advisory also includes a list of resources that organizations confronting cyber threats and evaluating cybersecurity best practices may find helpful, including StopRansomware.gov,[5] CISA's Ransomware Readiness Assessment,[6] CISA's cyber hygiene services,[7] and information about the U.S. Department of State's Reward for Justice Program.[8]

---

[4] https://www.cisa.gov/uscert/ncas/alerts/aa20-245a.

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

[6] https://www.cisa.gov/uscert/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat.

[7] https://www.cisa.gov/cyber-hygiene-services.

[8] https://rewardsforjustice.net/terrorist-rewards/foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/.