AN A.S. PRATT PUBLICATION
MAY 2017
VOL. 3 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 4 | MAY 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 [129] (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.

Ransomware Attacks Are on the Rise: Five Tips for Minimizing Risk

By Kenneth L. Chernof, Nancy L. Perkins, and Tiffany M. Ikeda*

The Department of Justice estimates that more than 4,000 ransomware attacks occurred per day last year. And the problem is only getting worse. The authors of this article explain ransomware, provide guidance on how to respond if you are a victim of a ransomware attack, and offer tips to minimize the risk.

Paying a ransom to access your computer files? Not as unusual as it sounds. The Department of Justice estimates that, on average, more than 4,000 ransomware attacks occurred per day last year. And the problem is only getting worse. According to Beazley,[1] a data breach response insurer, the number of ransomware attack claims the company received in 2016 was four times higher than 2015. This surge in ransomware attacks presents a serious, costly, and growing threat to businesses across all industries. Being educated on and prepared for such an attack is no longer an effort businesses can afford to sidestep.

WHAT IS RANSOMWARE?

Ransomware, as its name suggests, is a type of malware that holds a computer or computer files "hostage" until a ransom is paid. Ransomware is often delivered through malicious links, websites, or attachments. Unbeknownst to users who click on these links, websites, or attachments, malicious ransomware code quickly and quietly infects their computers.

Common variants of ransomware are lock screen ransomware and encryption ransomware. Lock screen ransomware works by locking a user's computer screen, preventing the user from accessing his computer. After the system starts up, the computer screen will display a threatening message, purportedly from a government agency, stating that the user has committed an illegal act and must pay a fine to regain access to his computer.

By contrast, encryption ransomware works by encrypting specific files—like Word documents and PDFs—rendering them inaccessible to anyone without the decryption

* Kenneth L. Chernof is co-chair of Arnold & Porter Kaye Scholer LLP's Litigation group focusing his practice on commercial, antitrust, and IP litigation. Nancy L. Perkins is counsel at the firm concentrating her practice on litigation, regulatory compliance, and consulting on emerging policy issues, with a principal focus on data privacy and security. Tiffany M. Ikeda is an associate at the firm representing businesses in a wide range of complex litigation, including in the areas of class actions, consumer protection, and regulatory compliance. The authors may be reached at kenneth.chernof@apks.com, nancy.perkins@apks.com, and tiffany.ikeda@apks.com, respectively.

[1] https://www.beazley.com/news/2017/beazley_sees_ransomware_attacks_quadruple_in_2016.html.

password. In both instances, the message is clear: pay up, usually in a difficult-to-trace digital currency like Bitcoin, or you will never see your files again.

RESPONDING TO A RANSOMWARE ATTACK

Should you give in? Well, that depends on a number of factors, including how badly you need access to your files. For businesses that have not taken preventative steps to backup data, ransomware can have a debilitating impact on a company's business.

In February 2016, Hollywood Presbyterian Medical Center fell victim to a widely publicized ransomware attack that seized control of its computer systems. Faced with the inability to access the hospital's records, Hollywood Presbyterian forked over 40 bitcoin (approximately $17,000) to the hackers. Allen Stefanek, Hollywood Presbyterian's chief executive, concluded that "the quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key." Healthcare providers are attractive targets for ransomware attacks because, in many instances, the loss of electronic patient medical records can create substantial risk to patient health. At that point, paying the ransom becomes a virtual necessity.

In Hollywood Presbyterian's case, paying the ransom "paid off"—the hospital regained control over its computer system. However, paying the ransom does not guarantee that you will regain access to your computer or files. According to Kaspersky Lab's 2016 Consumer Security Risks Survey,[2] approximately 36 percent of ransomware victims give in and pay the ransom, but 17 percent of those who pay never regain access to their files. Other times, after receiving the ransom payment, hackers demand even more money to provide the encryption key, or the victim regains access to its files, but then is immediately attacked again.

As a general matter, the Federal Bureau of Investigation ("FBI") does not support paying the ransom. Instead of paying up, the FBI recommends following these steps:

- Immediately contact your local FBI or U.S. Secret Service field office to report the ransomware attack.
- Implement your security incident response or business continuity plan, as it's important to take the necessary steps to ensure that disruption to the company's business is kept at a minimum. This may include retaining data security professionals to investigate the incident, as well as consulting with legal counsel to identify whether the attack triggers any obligations under federal and state data breach and privacy notification laws.

  In an interview with Arnold & Porter Kaye Scholer, FBI Special Agent Ray Martinez stressed the importance of implementing *and testing* a business

[2] https://press.kaspersky.com/files/2016/10/B2C_survey_2016_report.pdf?_ga=1.80392151.1709503615.1478184017

continuity plan: "Preparing for an unexpected event and actually practicing the recovery procedure, whether that be from a natural disaster or cyber threat, is a good way to determine what is business essential and what steps need to be taken to continue operations."

If you decide to pay up, Special Agent Martinez recommends verifying that the recovered data is not infected, then reimaging the system as soon as possible.

CAN YOU INSURE AGAINST IT?

Yes, ransomware attacks may be covered by your cyber insurance policy's "cyber extortion" coverage. Losses from ransomware attacks—including response assistance and any ransom paid to attackers—may be covered as cyber extortion-related costs. For coverage to kick in, some insurers may require that the policyholder first obtain their written consent before paying any ransom demand. And be mindful of policy deductibles. In a landscape where the average ransomware demand is less than $1,000, businesses with high policy deductibles may be stuck footing the entire bill. When in doubt, check with your insurer to verify your coverage.

FIVE TIPS FOR MINIMIZING RISK

In any event, the best defense to ransomware is to prevent an attack, or minimize the harm an attack could have on your business. Five steps management can take to proactively mitigate the risk of ransomware attacks are:

- *Backup your data and store it in a secure place.* In the event you become the victim of a ransomware attack, the backups will help mitigate the damage the attack will have on your business and may negate the need to pay the ransom altogether.
- *Patch your operating system, software, and firmware.* Hackers exploit vulnerabilities, so don't make it easy on them by keeping your system out-of-date.
- *Train your employees.* Make sure your employees understand what ransomware is so they can help protect the company's data. Employees should regularly backup their own data. They should also refrain from opening emails from unknown senders or downloading suspicious attachments.
- *Refresh your business continuity plan.* With ransomware attacks on the rise, your business should have a plan in place to keep operations running while responding to the crisis.
- *Review the U.S. Health and Human Services Office for Civil Rights Fact Sheet on Ransomware.* Even if you are not in the healthcare industry, this fact sheet provides guidance on how the implementation of certain security measures can help prevent ransomware infections and help maintain business continuity.