AN A.S. PRATT PUBLICATION
NOVEMBER - DECEMBER 2022
VOL. 8 NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 9** **November - December 2022**

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
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*, [8] 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

(2022–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.

Prepare Now to Manage Your Workforce Through a Cyberattack

By Brian M. Noh*

In this article, the author discusses preventative measures and contingency plans that businesses should adopt in advance of a cyberattack.

It is every employer's worst nightmare: an unsuspecting employee receives an email in the early morning from an individual claiming to be his supervisor. The email asks him to follow up on an urgent work assignment that needs his immediate attention. With multiple deadlines fast approaching, he does not think twice. He opens the email and attached file, and prepares to work. Within minutes, the entire system – including all confidential and proprietary data, timekeeping records, and payroll records stored in it – becomes inoperable and shuts down. The attacker delivers a single message to the employer: pay the ransom in exchange for the data or risk losing all the files.

Ransomware attacks are on the rise, and employers are increasingly being targeted. By some estimates, in the first seven months of last year alone, reports of ransomware attacks showed a staggering 62 percent year-over-year increase. Ransomware is a form of malicious software that can infect and lock down a target's network. While some malicious actors demand ransom in exchange for decryption software, others simply steal the company data regardless of whether a ransom is paid, often leaving victims with no way to tell what the attacker has accessed or taken. Needless to say, ransomware attacks can disrupt operations across the company and result in the loss of trade secrets, sensitive commercial information, personal data, and even medical documents.

More than ever before, it is imperative for employers to stay alert, understand the relevant laws, and implement both preventative measures and contingency plans.

FEDERAL AND STATE LAWS COUNSEL VIGILANCE

Ransomware attacks can instantly cripple a company's ability to manage its operations – payroll, timekeeping, and document retention – and the consequences can prove costly. In most states, payroll and timekeeping procedures are governed by both federal and state law. The Fair Labor Standards Act ("FLSA") is the primary federal law governing wage and hour standards for most workers in public and private employment. The FLSA does not require wages to be paid weekly or on a particular day of the month. However, once the employer designates specific payroll dates, it is required to adhere to

* Brian M. Noh, an attorney in the New York office of Akerman LLP, focuses his practice on labor and employment counseling and litigation. He may be contacted at brian.noh@akerman.com.

its schedule. Failure to do so can expose the company to claims for unpaid wages and, in some cases, liquidated damages.

Many states impose more stringent requirements. For example, in New York, manual workers must generally be paid on a weekly basis, while clerical workers must be paid at least semi-monthly. In California, employers are required to pay most non-exempt employees on at least a semi-monthly basis on designated paydays each month.

Employers are also required to implement compliant timekeeping practices. While neither state nor federal law generally require employers to use a particular method of timekeeping, companies must ensure that their system accurately, and reliably, records all hours worked, and that the underlying time records are preserved.

All employers are required to maintain payroll records for a minimum of three years under federal law. But some states may require companies to maintain records for a longer period. In fact, in most states, the best practice for employers is to retain payroll records for at least four years (up to six years in New York), and benefits-related documents for up to six years.

Importantly, the penalties for not maintaining accurate time and payroll records fall on the employer, not the employee. In litigation, an employee can prove unpaid wages through witness testimony, including their own self-serving testimony. The burden is then on the employer to establish the precise number of hours worked or to negate the employee's evidence. If an employer fails to produce the worker's payroll or timekeeping records, the case may very well be decided on the employee's own evidence.

DEVELOP A CRISIS MANAGEMENT PLAN

In today's digitized world, workforce management software and cloud-based services are becoming the new normal across public and private markets. Consequently, employers are well advised to implement both a contingency plan, and preventative measures, to respond to cyberattacks. Consider the following:

1. *Develop and test an incident response plan*. Time is of the essence in the minutes after a cyberattack. Make sure that your organization has developed a plan to respond to cybersecurity incidents and test the plan regularly. Among other things, the incident response plan should identify the employees who will be part of the incident response team and assign at least one person the responsibility to help the leadership navigate through the incident and, to the extent possible, mitigate any data losses as quickly as possible. Your plan should also define the payroll and timekeeping procedures that will be followed in the moments after a cyberattack. Most employers will need to have their employees temporarily switch to manual timekeeping or some other offline system. Discuss that system with your team, review it with all new workers as part of their onboarding process, and periodically go over it with your staff.

2. *Train and test your workforce on phishing*. Phishing refers to the fraudulent practice of sending emails to trick the recipient into revealing sensitive information or to deploy malicious software on a network. Many companies implement "simulated phishing" in the form of internal emails or urgent requests to provide targeted security awareness training. This can be a useful way of educating and training new and current employees on the latest cyber threats.

3. *Review your Services Agreement*. Many employers engage third party companies to process, manage, and store all of their timekeeping and payroll records. If that is the case for your company, review the services agreement with your payroll provider and clarify the scope of your company's, and the provider's, responsibility with respect to recording and storing personnel information. If you are not satisfied with those provisions, propose changes and negotiate an agreement that works for your organization.

4. *Build redundancy into your payroll system*. Understanding that cloud-based systems (or any electronic systems for that matter) are not perfect, employers should implement at least one or more backup recordkeeping systems. Consider backing up all personnel records in an alternate, encrypted, and offline system.

5. *Review and revise employee manuals/handbooks to address emergencies*. To the extent you have not done so already, revise your employee manuals/handbooks to describe how your organization will manage payroll and timekeeping, as well as any other personnel issues, in response to a cyberattack. If you are in a state that does not require payroll to be paid at statutorily defined intervals, add a disclaimer in your manuals/handbooks explaining that the payroll dates are subject to change in the event of an emergency, and that in such cases, payroll will be made on the next practically available day.

CONCLUSION

Ultimately, the effectiveness of a company's response will largely depend on its preparedness and dexterity in switching between different workforce management systems, as well as its understanding of its own limitations. In light of the increasing rate of cyberattacks, you should ensure that those plans have been thoroughly vetted and discussed with all decision makers, human resources, and information technology personnel.