AN A.S. PRATT PUBLICATION
JULY-AUGUST 2019
VOL. 5 • NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 6 JULY-AUGUST 2019

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 [171] (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

(2019–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.

Data Security Tips for Human Resources Professionals

David J. Oberly and Brooke T. Iley*

The task of securing company networks and systems is no longer delegated solely to an organization's IT department. Human resources plays an equally important role in protecting company data. The authors of this article explain how human resources personnel can serve as a robust line of defense against the unwanted intrusion into company networks and the theft of company data.

WannaCry and Petya are recent examples of ransomware attacks that shut down the networks and operations of companies across the world, causing millions of dollars in damages. The number of data breaches is skyrocketing, crippling all types of businesses—large and small, across all industries, and without regard to geographic boundaries. These attacks occur without warning, and in seconds can effectively hold all financial and business operations of a targeted entity hostage. In response, organizations are focusing on methods and practices to safeguard company data. The task of securing company networks and systems is no longer delegated solely to an organization's information technology ("IT") department. Human resources ("HR") plays an equally—if not more—pivotal role in protecting sensitive company data. Utilized properly, human resources personnel can serve as a robust line of defense against the unwanted intrusion into company networks and the theft of company data.

TODAY'S CYBERSECURITY THREAT AND THE ROLE OF HR

Gone are the days of paper files. While technology has transformed the way companies operate, this same technology has also opened the door to the significant and ever-growing threat posed by hacking and data theft. When it comes to cybersecurity, the biggest threat that companies face is not from malicious hackers, but rather from their own employees. In fact, the majority of data breaches arise from unintentional, non-employee errors, such as misplaced or stolen mobile devices and employees who leave passwords open to outside access. In addition to employee mishaps, an equally significant risk is posed by rogue employees who may, for one reason for another, intentionally misappropriate, misuse, or otherwise disseminate sensitive company data. Companies must guard against not only external data security threats, but also the data security vulnerabilities that exist within their organization as well.

* David J. Oberly is an associate at Blank Rome LLP representing clients in a wide range of complex cybersecurity and data privacy matters. Brooke T. Iley, a partner at the firm and co-chair of the Labor & Employment Practice Group, counsels and defends domestic and foreign corporations in all areas of employment and labor law compliance and litigation. The authors may be reached at doberly@blankrome.com and iley@blankrome.com, respectively.

Cybersecurity today requires much more than simply having the right technology in place to guard against data breach events. Moreover, cybersecurity is no longer the sole responsibility of an organization's IT department, as companies today simply cannot securely safeguard their sensitive, critical data through software and IT personnel alone. Given the significance of data security problems that originate internally as a result of the acts or omissions of a company's own employees, human resources professionals play a vital role in the protection of sensitive company data.

PRACTICAL TIPS FOR HR PROFESSIONALS

First, develop and implement data security policies and practices that address the current use of technology and data security within the organization. Do not rely on a policy written years ago that does not contemplate the actual operating systems and platforms used for modern day business operations. Creating a robust set of cybersecurity-based policies for employees is a simple yet effective way to combat data theft. As a general matter, these policies should define expectations for employees or anyone with access to firm data regarding issues such as the use of personal email and devices, file-sharing programs, the copying of data to personal devices, and the use of company systems from remote locations. In particular, there are several vital policies that should be included in all written cybersecurity plans. Of central importance is an up-to-date, detailed accessible use policy geared toward combating the inadvertent dissemination of company information by employees, which specifies the scope of activities that are allowable when utilizing company assets, including computers, smartphones, or any other device that can connect to company systems. In addition, mobile device policies—which specify the company's information security requirements for the safeguarding of confidential company information that is accessed or transmitted through any type of mobile technology—should also be included as part any comprehensive cybersecurity policy as well.

Training is another key area where HR can play a vital role in ensuring the security of company data and systems. Employees can be a formidable first line of defense against data theft, but only if they are informed about the vulnerabilities of company data and the significant interest that hackers have in getting their hands on sensitive company information. As a result, HR should include cybersecurity training as an integral part of the onboarding process. In doing so, employers should educate new employees on the company's security policies, procedures, and practices pertaining to the safeguarding of company information and data, and the consequences of failing to adhere to these standards. In addition, companies should complete additional cybersecurity awareness training on a regular basis for all members of the organization. In particular, employees should be educated on up-to-date, current methods that are being used by hackers to infiltrate company networks, such as social engineering fraud. Moreover, testing employees in real-life, non-classroom settings can be an

extremely effective training and educational tool. For example, HR can test employees by sending them simulated phishing emails to see if they are able to detect the malicious nature of the message. If they respond to the email, HR can then use this as an opportunity to educate the employee and further reinforce the importance of proper security measures and practices.

HR also plays a critical role in instilling and reinforcing a culture of cybersecurity throughout the workplace, which is key to ensuring data security, as cybersecurity awareness and training is only beneficial to a company if its workforce genuinely believes in and adheres to the practices and strategies that are provided to them. Here, HR professionals should focus on regularly communicating information and tips regarding critical data security issues throughout the organization, such as ensuring the security of mobile devices, maintaining strong passwords, and remaining cognizant of the ongoing threat of social engineering scams. HR can promote a culture of data security by both incentivizing proper data safety practices and, sometimes more importantly, disincentivizing data breach and theft scenarios, which can be accomplished by incorporating criteria relating to cybersecurity and data protection as part of employees' periodic performance evaluations and reviews.

Another important step that HR can take to further mitigate the risk of data theft is to tailor employees' access to electronic data to the worker's specific job duties. Strategically tailoring access is an effective way to prevent or limit internal employee data theft. Accordingly, HR professionals should work hand-in-hand with IT to ensure that employees only have access to information and data that is essential to the duties and responsibilities of their position within the company. In addition to limiting what data is accessible, companies should also monitor what data is being accessed on the company's network. Data monitoring can not only detect leaks when they happen, but can also discourage employees from taking unnecessary risks by sharing firm data. In particular, HR and IT should monitor electronic usage to identify any early warnings of potential vulnerabilities with an eye toward unusual activity, particularly if information is being pulled off of a company's network.

Similarly, in addition to monitoring data, HR should also monitor employees for potential data security threats as well. As a starting point, HR should conduct thorough background reviews of all candidates for employment before the time they are hired. Background checks are extremely useful because they can identify any prior fraudulent or dishonest activity on the part of the potential new hire, which is a clear red flag that the individual may pose a data security threat if employed by the organization.

In addition, protective monitoring of current employees by HR is also necessary to reduce opportunistic or counterproductive behavior by employees. As one of HR's primary functions is to understand employee behavior, a company's HR team is in the best position to identify potential early warning signs that an employee could be headed in the wrong direction, or laying the groundwork to improperly disseminate

or steal company information. The best way to identify these high-risk employees is to observe their behavior. Being hostile to managers and fellow employees, and severe dips in performance, are tell-tale signs that an employee might pose a threat of compromising company information and data. After a high-risk employee is identified, HR should guard against the increased threat of data leakage or theft by engaging in increased data monitoring of the employee. In particular, companies should monitor for large file transfers and any uptick of emails being sent to the employee's personal email address, which are often red flags for improper data handling practices. Importantly, however, it is imperative that all background reviews and employee monitoring activities are carried out by the company in accordance with all legal requirements and regulations.

Finally, any time an employee leaves the company, HR should implement proper offboarding procedures to limit the potential for data leakage. In this regard, HR should utilize exit interviews as an opportunity to repossess company data from all of the departing employee's electronic devices and to reaffirm and reemphasize the employee's ongoing data protection obligations, which continue even after the employee severs his relationship with the organization (including any contractual obligations the employee may have). In addition, HR should immediately remove an employee's access to the company systems and data, and change all passwords, as soon as a worker departs the company. In the event HR decides to terminate an employee, it is imperative that this is done prior to the time the worker is notified of his or her termination.

THE FINAL WORD

No longer is it safe to think your organization's IT department is responsible for ensuring the security of company networks and data. HR plays a critical role in that effort as well. As the number and severity of data breaches continues to climb today with no foreseeable end in sight, now more than ever HR professionals must be proactive in implementing effective policies, procedures, and practices to mitigate the data security risk posed by a company's own employees. Through the implementation of several key cybersecurity measures and safeguards and the utilization of an overall cybersecurity risk management program, HR professionals can serve as a pivotal player in effectively minimizing the risk faced by organizations today of falling victim to a catastrophic data breach.