AN A.S. PRATT PUBLICATION
JANUARY 2018
VOL. 4 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 1 | JANUARY 2018

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (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

(2018–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.

Cybersecurity Risks in the Workplace: Managing Insider Threats

By Lindsay Burke and Moriah Daugherty*

One of the most critical risks a company can face is the cybersecurity risk associated with its own employees or contractors. To guard against these risks, companies can implement various policies and procedures to address risks throughout an employee's tenure, from pre-hiring to post-employment, and can implement many of these same precautions with respect to contractors, consultants, or any other third parties with access to company systems. The authors of this article explain how employers can manage insider threats.

Today, one of the most critical risks a company can face is the cybersecurity risk associated with its own employees or contractors. Companies are confronting an increasingly complex series of cybersecurity challenges in the workplace, including employees failing to comply with established cybersecurity policies; accidentally downloading an attachment containing malware or providing their credentials in response to a phishing scam; or intentionally stealing company information for the benefit of themselves or the company's competitors — for example, by simply copying information to their email or a thumb drive and leaving the company. Contractors or consultants with access to company systems can pose these same challenges. To guard against these risks, companies can implement various policies and procedures to address risks that may arise during an employee's tenure, from pre-hiring to post-employment, and can implement many of these same precautions with respect to contractors, consultants, or any other third parties with access to company systems.

POLICIES AND PROCEDURES TO PROTECT EMPLOYERS

Before hiring employees or contractors, companies can ensure they have in place policies and procedures to protect themselves. Particularly important policies include:

- acceptable use of electronic devices and systems;
- mobile device;
- data collection and retention;
- notice and consents for monitoring and collection of information on company systems; and

* Lindsay Burke, a partner at Covington & Burling LLP, is vice chair of the firm's employment practice group and regularly advises U.S., international, and multinational employers on employee management issues and international human resources compliance. Moriah Daugherty is an associate at the firm advising clients on a broad range of cybersecurity, data privacy, and national security matters. The authors may be contacted at lburke@cov.com and mdaugherty@cov.com.

- background check policies that permit pre-employment and ongoing vetting of all employees.

Companies should enact enhanced screening and background checks for new hires who will have access to the company's "crown jewels" and systems that can connect to or access the same, and should require third parties that provide contractors to demonstrate that they are meeting the company's standards for screening and background checks.

When drafting policies, companies should ensure all important stakeholders—including human resources, information technology, and legal—provide coordinated input. Companies should also ensure that all employee-related policies are aligned with other company policies, particularly data security and cybersecurity policies, including the company's incident response plan.

When onboarding employees, companies should use procedures including training, policy review, and obtaining key acknowledgements and consents to establish a culture of awareness and compliance. It is particularly important for companies to complete the following tasks during employee onboarding:

- apprise new employees of the company's expectations regarding protection of confidential information and critical infrastructure (including ensuring that no new employee has brought any confidential information from another company with them);
- provide a briefing of policies governing employee access to information and those that could implicate employees' privacy;
- notify employees that they have no expectation of privacy if using personal devices for business purposes; and
- obtain employee consent to any applicable monitoring.

Employees should be asked to execute a non-disclosure agreement and other documents that protect the company's information, and the executed copies of these documents should be safely stored in the company's personnel file or human resources system.

Companies can and should also implement parallel procedures for outside directors, vendors, contractors, and third parties with access to company networks and systems.

EMPLOYERS MUST REGULARLY ASSESS INDICATORS OF ANY POTENTIAL ISSUES

After employees begin work, companies should regularly assess indicators of any potential issues, including by reviewing:

- any unusual systems accessed by employees;
- what documents and information employees are downloading, printing, or emailing;

- when employees are performing actions on company systems; and
- any efforts by employees to exceed access privileges or records of failed log-in attempts.

Conducting real-time monitoring of employees has significant privacy implications, particularly outside the United States. As a result, a company will typically want to notify employees of the monitoring and obtain prior consent or acknowledgement that an employee's use of the system constitutes consent to the interception of their communications and the results of such monitoring may be disclosed to others, including law enforcement.

Companies should conduct regular, required training with employees concerning cybersecurity risks, including the risks associated with phishing attacks and fraudulent email solicitations. In addition, companies should make sure that compliance with security policies is included as a metric in performance evaluations for employees, particularly those employees with access to business critical information.

These same procedures should be in place for contractors, consultants, or any other third parties who have access to company systems and information. If necessary, companies should review the contracts they have in place with vendors or staffing agencies to ensure that proper procedures, including applicable acknowledgments and consents, are in place.

IF AN EMPLOYEE IS POTENTIALLY DISGRUNTLED OR AN INSIDER THREAT

If a company believes an employee is potentially disgruntled or is an insider threat, the employee's manager should coordinate with other departments—including legal, human resources, and information technology—to obtain additional information and plan a course of action. Investigations can include forensic computer or network searches, preservation of affected systems, and interviews with employees. While developing the facts, a company should consider when or how to suspend or revoke a suspected insider threat's access or take additional action against the insider—though companies should beware that taking action against a suspected employee is likely to implicate employment laws in the United States or elsewhere.

OFF-BOARDING EMPLOYEES

When off-boarding employees, companies should take steps to protect themselves. It is imperative for companies to develop policies and procedures for off-boarding employees that are directed at minimizing risks of data leakage. Exit interviews should be conducted wherever possible; they will allow companies to spot potential problems or identify red flags.

When an employee resigns, a company should decide whether to institute a protocol to remove or limit the employee's access to confidential information even before an employee's last day at work. Human resources should work with information technology to audit the employee's most recent network access and email activity to ensure the employee has not harvested any confidential information.

When the company is preparing to terminate an employee, the company should implement a protocol to protect company confidential information, including removing an employee's access to networks and systems before or simultaneously with notifying the employee of the impending dismissal. The same should be done when a contract with a consultant, vendor, or contractor is nearing its end.

All employees who leave the company and all contractors whose contracts end should be reminded of ongoing obligations to protect the confidential information of the company. They should also be asked to return all company information, documents, and electronic equipment before their last day at work.

CONCLUSION

Employees can present a significant threat to a company's business critical information, as can contractors or consultants with access to company systems. Companies should ensure that relevant departments within the company, such as legal, human resources, and information technology, are coordinating to take steps to protect the company against such threats, including those set forth above.