AN A.S. PRATT PUBLICATION
APRIL 2019
VOL. 5 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 3 | APRIL 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 [69] (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.

Lessons in Data Protection and Cybersecurity in M&A

Cynthia J. Cole, James Marshall, and Sarah J. Dodson*

Companies engaging in mergers and acquisitions are looking for growth and revenue and a data security incident after the fact is a very unwelcome surprise. The authors of this article provide guidance that may help prevent or minimize the adverse consequences of a data security breach.

Data privacy, protection, security policies, and procedures have moved squarely into the governance spotlight. Boards of directors and senior management are increasingly focused on data privacy, as are customers, employees, and shareholders. And the frequency of high-profile data security incidents emphasizes the necessity of implementing data privacy and security policies and procedures in connection with both the mergers and acquisitions ("M&A") process and the satisfaction of compliance and disclosure obligations.

In 2018, companies have had to come to grips with wide-ranging data protection legislation. The data landscape has changed quickly, and some companies have had to face some very difficult lessons. Many of those lessons have been through data security incident disclosure and regulatory authorities have not failed to notice. Those regulatory authorities are paying increasing attention and are showing a willingness to approach record numbers in fines. On February 21, 2018, the Securities and Exchange Commission (the "SEC") issued updated interpretive guidance to assist public companies in preparing disclosure regarding potential cybersecurity risks and incidents.[1] The European Union's General Data Protection Regulation (the "GDPR") went into effect on May 25, 2018, codifying compulsory security practices, disclosure, accountability, and transparency obligations for multi-national organizations and companies with operations that touch Europe. Individual states and local municipalities are even flexing regulatory muscle in this space; most recently, the California Consumer Privacy Act of 2018 (the "CCPA") was signed into law on June 28, 2018, giving individual residents in California broad rights with respect to the nature and use of their personal information by corporations and a private right of action for a data breach.

* Cynthia J. Cole (cynthia.cole@bakerbotts.com) is special counsel at Baker Botts L.L.P. representing global companies and private equity funds in complex strategic transactions, with a focus on technology and cross-border transactions involving data privacy, data sharing and information privacy matters. James Marshall (james.marshall@bakerbotts.com) is a corporate partner at the firm representing public and private companies in a broad range of corporate and securities matters. Sarah J. Dodson (sarah.dodson@bakerbotts.com) is a corporate associate at the firm representing public and private companies in mergers and acquisitions, public and private securities offerings, and general corporate concerns.

[1] *Available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

While regulatory bodies heighten their focus on cybersecurity, public companies are increasingly data breach targets. In addition to efforts to improve data security practices and to comply with regulatory requirements, there are a number of specific best practices for companies to consider as they engage in M&A activity.

M&A DUE DILIGENCE

Data and the security of data has not always been a standalone consideration in M&A due diligence. Lawyers historically asked a series of routine, privacy-related questions of a company and cybersecurity concerns were often embedded in questions about other risk areas. More recently, there has been significant attention paid to the risks associated with data breaches, but less has been known about how best to uncover these risks and liabilities.

As part of its efforts to uncover potential cybersecurity risks or incidents at a target, some key areas for an acquiring company to direct its focus include:

- *IT and data assets*: What IT assets, systems, software, platforms, websites, and applications exist and are critical to the target? How is company data stored, and is it encrypted?
- *Governance practices*: Who has responsibility for privacy compliance and data security within the company and for overseeing security preparedness? Is there a specifically appointed data protection officer?
- *Security risk management*: What is the target's data security infrastructure? Has the target experienced any interruptions, outages, or suspensions of system operations? Does the target have a comprehensive written security management program and show proof of vulnerability testing? Consider hiring an outside firm to do penetration tests or security audits.
- *Insurance*: Does the target have data security insurance coverage? Does the target require vendors to maintain such coverage?
- *Historic incident or loss experience*: Has the target received complaints from customers, employees, contractors or other third parties regarding data privacy and security practices? Have any such complaints resulted in litigation or other proceedings?
- *Sharing information with third parties*: How does the target vet third party security infrastructure, policies and records? Does the target ensure audit rights in contracts with third parties? Has the company assessed its obligations to notify customers and regulators in case of a breach?

Ultimately, while these examples provide a starting point for appropriate cybersecurity diligence, it is critical that the acquiring company tailor its diligence on data privacy and security matters to the target company.

POST-ACQUISITION INTEGRATION

A fulsome diligence effort focused on data privacy and security matters should be designed to prevent the unfortunate situation where an acquiring company learns of ongoing data breaches at the target company after the transaction has closed. Even with heightened awareness and diligence, efforts to uncover cybersecurity weaknesses prior to closing the acquisition may prove unsuccessful, and so organizations should prioritize efforts to learn of any existing breaches during the integration process. Measures should be targeted to the specific risks faced by the target company but may include having the target company adopt the acquiring company's existing cybersecurity policies, performing a risk assessment to determine the adequacy of the target company's cybersecurity measures and implementing training programs to ensure knowledge across the target company's key personnel.

DISCLOSURE

Finally, companies must remain mindful of key disclosure requirements and ensure that they are responsive to such requirements in an actively changing regulatory landscape. The SEC's February 2018 guidance recognizes that immediate disclosure of a data security incident may not be appropriate, but also stresses that "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures." While this may seem to provide some comfort with respect to the timing of U.S. disclosure requirements, companies must continue to pay close attention to how a breach may impact their filing obligations, including which filings are implicated. A material data security breach may trigger an obligation to file a Current Report on Form 8-K (including if the issuer has a duty to correct prior disclosure) and should also be evaluated in connection with the preparation of Annual Reports on Form 10-K or 20-F and Quarterly Reports on Form 10-Q.

While the SEC provides some flexibility in timing disclosure depending on the facts and circumstances of the breach and any related investigation, the GDPR takes a strict approach, requiring disclosure to the relevant European Union authority no later than 72 hours after the data breach is confirmed – a tight timeframe when a company is in the throes of investigating the extent and severity of the issue. Failure to notify authorities or individuals within the deadline may result in significant fines and subjects the company to widespread multi-jurisdictional litigation. Ultimately, in the event of a material data security breach, the GDPR aligns with the SEC guidance in that public disclosure will, sooner rather than later, be necessary.

In order to comply with regulatory requirements and avoid fines or enforcement actions, companies are encouraged to maintain an incident response plan that identifies a response team, key timing factors, and a sequence of action items in the event of a breach to help analyze what notifications and disclosure requirements apply. In addition, a well-formulated response plan should include implementing blackout periods

when appropriate while investigations of cyber security incidents may be pending. The SEC flagged this as an important consideration, noting in their February 2018 guidance that "companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material."

CONCLUSION

Data security is key. Companies engaging in M&A are looking for growth and revenue and a data security incident after the fact is a very unwelcome surprise. Data security should be a dynamic area of focus in both the diligence and integration process. It should be tailored to the target and the risk and should not be taken lightly. Establishing strong practices in each of these areas, as well as regulatory and compliance policies that are regularly updated as regulations evolve, can help prevent or minimize the adverse consequences of a data security breach.