AN A.S. PRATT PUBLICATION
OCTOBER 2017
VOL. 3 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 8 | OCTOBER 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) 487-3385
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 [272] (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.

ACC Cybersecurity Guidelines: The What, Why, and How

By Stephen E. Reynolds and Nicole R. Woods*

In response to the increased concern surrounding cybersecurity, the Association of Corporate Counsel has released the Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information. *The authors of this article discuss the guidelines, which can serve as a benchmark for law firm cybersecurity practices.*

More and more frequently, headlines are filled with news of crippling cyberattacks designed to cause the most chaos in the shortest amount of time. Recent examples include the WannaCry and Petya ransomware attacks that affected businesses worldwide, including many law firms. The WannaCry attack affected more than 230,000 computers in more than 150 countries within a single day, causing massive disruptions.

According to the 2016 TechReport issued by the American Bar Association, 20-25 percent of law firms have already experienced a data breach. In fact, one large law firm, which recently touted its cybersecurity expertise, was hit by the Petya attack and suffered several days of total system shutdown. It is no surprise, therefore, that two-thirds of chief legal officers and general counsels rank information privacy and protection of corporate data as "very" or "extremely" important.

In response to the increased concern surrounding cybersecurity, the Association of Corporate Counsel ("ACC") released the *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*.[1] The ACC hopes these guidelines will serve as a benchmark for law firm cybersecurity practices.

ARE THESE GUIDELINES THE NEW STANDARD FOR OUTSIDE COUNSEL?

Although the ACC intends for the guidelines to "offer in-house counsel a streamlined and consistent approach to setting expectations with respect to the data security practice" of outside counsel, the ACC repeatedly cautions that the guidelines should not serve as an industry standard. It specifically provides that the guidelines are not

* Stephen E. Reynolds, a former computer programmer and IT analyst, is a partner in Ice Miller LLP's Litigation Group, and co-chair of the Data Security and Privacy Practice, focusing his practice on commercial litigation and data security and privacy law. Nicole R. Woods is an associate the firm's Data Security and Privacy Practice, focusing on complex commercial litigation, including contract disputes, business torts, and financial services litigation. The authors may be reached at stephen.reynolds@icemiller.com and nicole.woods@icemiller.com, respectively.

[1] http://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf.

intended to "substitute for corporate counsel's own legal analysis and good judgment" and they are "not intended to establish any industry standards for any purpose for either the company client or outside vendor."

Although ACC goes out of its way to hopefully avoid setting minimum standards, the guidelines themselves read like a contract, requiring that outside counsel "shall" complete certain tasks and meet certain standards.

WHAT DO THE GUIDELINES SUGGEST?

The guidelines set out a framework of various requirements in the hopes that outside counsel will ensure appropriate technical and organizational measures for protection of the client's company confidential information and other similar data. Confidential information is broadly defined and includes items such as employee personally identifiable information, information relating to the company's physical or cyber security measures, material non-public information (for publicly traded companies), and protected health information.

Outside counsel may already satisfy some of the more routine guidelines as part of their current operating procedures. For example, outside counsel must return or destroy company confidential information at the conclusion of the engagement unless required to maintain the information by law. Outside counsel must also continually monitor networks, employees, and subcontractors for malicious activity or activity that may damage the company's confidential information. Additionally, they must perform assessments on their systems to minimize security vulnerabilities. Law firms likely already have some sort of system or policy in place to satisfy these requirements or are in a position where they could quickly and easily implement the solutions.

Additionally, outside counsel may already meet the requirement that they install and utilize consistently updated antivirus protection, install routine software patches, and maintain firewalls or other network protections. The guidelines also require outside counsel to have application security and software controls to minimize system and network vulnerabilities. Finally, outside counsel may also already satisfy the requirement that the firm manage access to the company's confidential information, such as limiting access to the information to only certain individuals or certain job functions. Many document management systems provide this functionality, and it is easy to implement.

Two of the guidelines that speak to administrative matters may be either new to outside counsel and/or more burdensome to actualize. First, the guidelines provide that outside counsel will obtain and maintain cyber liability insurance with a minimum coverage level of $10,000,000. A LogicForce study released in June 2017 stated only 23 percent of law firms currently carry cybersecurity liability insurance. However, the policies can provide significant benefits, including coverage for damage to data, disruption of business, and reputational harm.

Second, companies may request that outside counsel undertake the process to obtain ISO27001 certification for its information security management system. This type of certification results from a framework of policies and procedures that include controls for legal, physical, and technical aspects of the system. Obtaining this type of certification can take significant time and can result in significant costs.

The remaining guidelines fall into one of two categories: data handling or physical security.

Data Handling

When many people think of cybersecurity, they think of encryption. The guidelines are no different. They first focus on encryption in transit. This guideline is uncharacteristically vague. Rather than providing specific encryption requirements, it simply provides that when transferring company confidential information and communicating with the company, outside counsel will use encryption based on guidance provided by the company. This guideline seemingly leaves encryption of email and other communications up for discussion between the company and outside counsel.

For encryption of data at rest—data not moving through the network—outside counsel must encrypt all company confidential information that resides on any server, computer, or back-up tape. Unlike the guideline for encryption in transit, this guideline specifically requires that counsel use encryption solutions certified against U.S. Federal Information Processing Standard 140-2, Level 2, or an equivalent industry standard. The guidelines also provide the same encryption standard for confidential information that resides on or is transferred to mobile devices, removable media, tablets, and laptops.

In the event a data breach does occur or is suspected to have occurred, the guidelines require that outside counsel notify the company within 24 hours of discovering the actual or suspected breach. After notification, outside counsel must also provide companies with access to an individual who will act as the single point of contact on a 24/7 basis for the company for purposes of addressing the breach.

Physical Security

Generally speaking, the guidelines require company confidential information to be physically secured against unauthorized access. For law firms that host the confidential information on their own systems and servers, there are many more requirements, and this may be an area where outside law firms fall short of the guidelines.

Outside counsel must implement *at least* 12 separate physical security precautions, including:

(1) 24/7 security guards monitoring the entrance to the facility(s) where the confidential information is stored, accessed, processed, or destroyed;
(2) camera surveillance with active monitoring;

(3) no exterior access points; and
(4) enhanced access to computer rooms such as palm readers, iris recognition, or fingerprint readers.

Smaller law firms that host their own data likely do not currently have these protections in place.

HOW CAN LAW FIRMS IMPLEMENT THE GUIDELINES, AND ARE THERE ANY ADDITIONAL FACTORS TO CONSIDER?

Some law firms may already satisfy one or more of the guideline requirements. Others may feel overwhelmed by the seemingly daunting steps they need to take in order to comply. In any case, there are steps firms can take in order to implement the guidelines, as well as additional considerations firms must take into account when formulating their implementation plans.

Firms can add a chief information security officer ("CISO") to the payroll. A CISO can be responsible for establishing and maintaining an implementation strategy and is well-versed in the technological aspects of compliance. This allows the attorneys to focus on practicing rather than technical IT matters. As part of this, firms may also consider creating and maintaining a firm-wide and client-wide cybersecurity protocol based on the guidelines. That would eliminate the need, to a large extent, to create individual protocols for each client.

Firms should make sure antivirus software is used and is updated daily for malware definitions. Other security software, such as a firewall, should also be implemented. Firms can also obtain cybersecurity insurance policies, which the American Bar Association began offering in February of this year.

Firms will also need to assess their current system for available encryption methods, including those available for email and other communications. Separate and apart from the ACA guidelines, the ABA has recently provided ethical guidance concerning protection of client communications in Opinion 477R, issued in May 2017.[2] Previously, the ABA's Opinion 99-413 concluded that use of unencrypted email is a reasonable means to maintain client confidentiality. Opinion 477R, however, now concludes that "it is not always reasonable to rely on the use of unencrypted email." Instead, counsel should make "reasonable efforts to prevent the access or disclosure" of the client's information.

What constitutes "reasonable efforts" on the part of counsel is not a matter of black and white. The Opinion does not provide a toolkit for counsel to utilize in order to ensure proper protection of information. Instead, the Opinion explains that counsel

[2] https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA Formal Opinion 477.authcheckdam.pdf.

should complete a fact-based analysis in determining what constitutes "reasonable efforts" by considering the factors set forth in Comment [18] to Model Rule 1.6(c). Those factors include, among others, the sensitivity of the information and the likelihood of disclosure. The Opinion specifically states this fact-based analysis "means that particularly strong protective measures, like encryption, are warranted in some circumstances." In addition, the Opinion makes clear that in order to satisfy the duty of competency, attorneys must stay abreast of the benefits and risks of relevant technology.

A firm may choose to simply send sensitive information in an encrypted email when communicating with a client. There are several solutions on the market for both small and large firms to implement such a plan. Some allow the user to choose when to encrypt an email or can automatically encrypt emails if the email or attachments meet specific user-set criteria.

However, even when sending an encrypted email, the metadata of the message—such as sender, recipient, subject line, time, and date—may remain unencrypted and open to prying eyes. In addition, if using a secure web-based email provider such as Gmail or Yahoo, the email provider still retains a copy of the entire communication, not just the metadata, and the message will remain vulnerable to possible collection by government or law enforcement. Firms may instead choose to communicate with companies via a secure web portal, which allows for complete protection of the communication from all possible interceptors. All client communications are created and retrieved within the portal, and the entirety of the message, including its metadata, is encrypted. Email is utilized to notify the message recipient that he or she received a new message in the portal, but the message itself if not sent via email. This process is somewhat time consuming for both the firm and the client, but it is one solution to protect highly sensitive communications.

Finally, in order to address other security measures, law firms that host their own data may consider migrating their information to the cloud, which would place the data in a vendor's data center. Data centers offer both public and private clouds depending on the need of the firm. In both situations, the firm's data is completely segregated. However, with a public cloud, multiple companies share the same set of servers. With a private cloud, however, the company's data is contained on an entirely separate hardware that is not shared. Using a data center can help with the physical security guidelines, because it often has the security and supervision the guidelines require.

Cloud computing is relatively new in the legal world, and many firms are hesitant to relinquish control of their data. However, of the 20 states that have reviewed cloud computing from an ethics and confidentiality standpoint, all 20 found that cloud computing is permitted with reasonable care.

In the end, each law firm may choose to conduct its own risk assessment to decide how best to comply with any ethical or client responsibilities for protection of data.