AN A.S. PRATT PUBLICATION
JUNE 2017
VOL. 3 • NO. 5

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

# Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 5 | JUNE 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 [159] (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.

# Managing Cyber Risks: Tips for Purchasing Insurance That Works for Your Business – Part II

***By Omid Safa, James S. Carter, and Jared Zola****

*This article highlights several strategies for maximizing the value of a cyber insurance purchase. The first part of the article, which appeared in the May 2017 issue of* Pratt's Privacy & Cybersecurity Law Report*, highlighted the need for an organization to reevaluate its insurance coverage as part of a comprehensive strategy for addressing emerging cyber risks and outlined several "big picture" considerations relevant to any organization contemplating a cyber insurance purchase. This second part focuses on several strategies to consider when negotiating a cyber insurance purchase and seeking to customize the policy to align with an organization's particular business needs.*

## LOOK BEYOND YOUR IMMEDIATE CONCERNS

Performing a holistic risk assessment involving input from a cross-functional team is a critical first step when contemplating any cyber insurance purchase. Performing such an analysis will allow the purchaser to identify the particular risks and losses facing the business, prioritize among those threats, and pinpoint the specific items that "must" be covered to ensure that a cyber insurance purchase provides meaningful protection and value to the organization. But the intricacies associated with a detailed (commonly technical) risk assessment should not be confused with the language you ultimately need in your cyber insurance policy. The specific risks and losses identified in the risk assessment merely serve as guideposts and reflect the starting point when evaluating proposed policy language. Instead, negotiating policy language that covers not only your immediate concerns – but provides the *broadest overall* coverage possible – should always be the goal when purchasing cyber insurance for your organization.

## WHEN TO USE GENERAL VERSUS SPECIFIC LANGUAGE

Negotiating the most favorable policy possible is rarely a matter of simply including specific language corresponding to the list of items identified in your risk assessment. Indeed, taking such an approach often backfires and leaves the purchaser with significantly less coverage than it could have obtained. Remember the structure of an insurance policy. Like a funnel, a policy opens with insuring agreements that prescribe the outer bounds of coverage. The coverage is then methodically whittled down by a series of limitations and exclusions found elsewhere in the policy. All too often,

* Omid Safa is an associate, James S. Carter is of counsel, and Jared Zola is a partner in Blank Rome LLP's policyholder-only insurance coverage practice. The authors may be contacted at osafa@blankrome.com, jscarter@blankrome.com, and jzola@blankrome.com, respectively.

purchasers focus solely on the latter provisions when negotiating policy language and attempt to address coverage for their "must have" items through *specific* caveats and exceptions. Such an approach seldom secures the most favorable policy language for an organization.

Ultimately, the coverage available can only be as broad as the breadth of the language used in the insuring agreements. Accordingly, policyholders should seek to negotiate broad insuring agreements using *general* terms that are expansive enough to address any pressing concerns while remaining flexible enough to respond to unknown threats. This approach better positions a policyholder with respect to unforeseen risks and ensures that any "upside" implicit in the policy language inures to the policyholder's benefit. Conversely, demanding over specificity in insuring agreements tends to narrow protection and restrict the items eligible for coverage from the outset.

Purchasers should generally reserve such specificity for exclusions and limitations. The use of more specific language can help "pin down" such provisions by narrowing the circumstances trigging their application. Of course, there may be circumstances when a degree of specificity is necessary in an insuring agreement to accomplish certain objectives and satisfy certain stakeholders. For example, contractors are often required to purchase cyber insurance that "explicitly" references certain types of risks. Purchasers should be strategic and take care to strike the right balance in those instances. While some specificity may be just what the doctor ordered, an overdose will do more harm than good. Knowing where to draw the line is an art that comes with experience.

## ENSURE ALL COVERAGE PARTS ARE SYNCHRONIZED

A cyber-related event will typically lead to two types of losses for a policyholder: (1) first-party losses and (2) third-party losses. Generally speaking, first-party losses are the direct losses a policyholder suffers as result of a cyber event. For example, such losses can include the policyholder's costs in direct response to the event (e.g., investigation costs, remediation costs, public relations expenses, notification costs, and credit monitoring fees) and the policyholder's loss of business income as a result of the event (e.g., a network interruption). By contrast, third-party losses are the losses incurred as a result of claims and lawsuits brought against the policyholder by individuals and entities alleging harm caused by a cyber event.

For obvious reasons, a policyholder will often incur first-party losses well before it faces third-party claims in connection with a cyber-related event. In light of this, it is important to make sure that the first-party coverages and the third-party coverages in your cyber policy are synchronized and work together to provide fulsome protection for both types of losses. In particular, purchasers should avoid trigger language, interrelated act provisions, and notice requirements that create unnecessary tension between the coverages and fail to account for the inherent lag in the timing of first-party and third-party losses. For example, a policy should never interrelate first and

third-party losses when the first-party coverage is tied to the timing of an occurrence and the third-party coverage is claims made. Such inconsistencies are traps for the unwary and merely lay the groundwork for future disputes.

Policyholders should also avoid terms that seek to condition first-party coverage on the fulfillment of requirements that risk prejudicing the policyholder's defense of third-party lawsuits arising from the same event. For example, some policies require a policyholder to submit a detailed proof of loss and sit for an examination under oath shortly after providing notice of a cyber event as a prerequisite to obtaining first-party coverage. But disclosing such details may ultimately exacerbate the risks to a policyholder by generating records and transcripts that can be mined by claimants in future lawsuits. Both the policyholder and the insurer have an interest in avoiding such disclosures. Proof of loss provisions should be tailored with respect to timing, specificity, and scope to prevent compromising a policyholder's defense and protect any privileged information from the claimants and their lawyers.

## AVOID UNINTENDED CONSEQUENCES

Throughout the negotiation process, a purchaser should bear in mind that in the event of a coverage dispute, the insurance policy will be interpreted as a whole and all distinctions in the policy language will be given meaning. Thus, it is important to refrain from considering proposed changes in isolation. Rather than focusing solely on the provisions immediately impacted by a proposed change, a purchaser should consider whether the proposal has other implications that may undermine the overall coverage afforded. Even seemingly minor changes can have ripple effects across the insurance policy and lead to unintended consequences that are detrimental to the policyholder.

Such ripple effects are far more likely to be coverage reducing given the dynamics involved when negotiating with insurers. Purchasers should not lose sight of the fact that insurers are repeat players when it comes to negotiating modifications to their off- the-shelf cyber forms. The underwriters will be well-versed in the ins and outs of the policy terms and conditions and how they interact with one another (and have the help of the insurer's counsel when considering any new wrinkles). Consequently, risk managers should strongly consider enlisting the assistance of outside counsel to vet all proposed changes and ensure that the final insurance policy is free of any unpleasant surprises.

In any event, it is paramount for a purchaser to closely scrutinize any proposed changes to determine the total impact on coverage. This is especially important when considering any edits that an insurer makes in response to requests for broader coverage. Unfortunately, when left unchecked, insurers routinely purport to "accommodate" such requests by proposing changes that are ostensibly responsive, but ultimately lead to a reduction in total coverage. Thus, purchasers must take care to ensure that changes are truly additive and not merely the sleeves off their vest or, worse, a veiled attempt at lessening coverage elsewhere in the policy.

## PUSHBACK ON EXCLUSIONS AND LIMITATIONS

Cyber insurance policies often feature a combination of exclusions and limitations drawn from other types of policies as well as newfangled exclusions unique to cyber insurance. Such provisions do not always mesh well with the purpose of cyber insurance and, in some instances, may actually be more restrictive than the traditional versions of the exclusions found in other types of policies. For example, insurers often dispense with common exceptions and caveats when adding traditional exclusions to cyber insurance.

Consistent with the ongoing development of cyber insurance, some cyber insurance policies appear to be testing new exclusions unique to cyber and privacy incidents. These exclusions are often unusually worded and leave purchasers scratching their heads as to how they may apply. Such exclusions generate uncertainty, lay the foundation for future coverage disputes, and should be avoided. Counsel can help purchasers scour policy forms for exclusions and limitations that are too draconian and need to be rectified before completing a cyber insurance purchase.

## MAINTAIN PRIVILEGE OVER YOUR STRATEGIC DELIBERATIONS

Experienced brokers can provide helpful insights during the purchasing process due to their knowledge of the marketplace and their ongoing working relationships with many insurers. Depending on the jurisdiction, however, communications with a broker may not be protected from disclosure in a subsequent coverage dispute. Purchasers should take special care to preserve privilege with respect to attorney-client communications and strategic advice in jurisdictions where such protection does not extend to brokers. Among other things, purchasers should consider limiting a broker's access to written work product and attorney-client discussions evaluating the legal effect of proposed policy language in order to preserve all privileges and protections. After conferring with counsel and evaluating the proposed policy language in light of the advice received, the purchaser can reach a decision regarding any necessary changes and separately communicate them to the broker without divulging the underlying legal advice.

## ENSURE THAT POLICY CONDITIONS ARE ALIGNED WITH YOUR BREACH RESPONSE PLAN

Your breach response plan is your roadmap for navigating a cyber-related event when the pressure is on. Making certain that the conditions in your cyber policy are properly aligned with your breach response plan is critical to coming through that difficult time unscathed. For example, if your current response plan contemplates predominantly internal response and remediation efforts, or the help of a particular outside consultant, such considerations should be kept in mind when

evaluating insurance options and negotiating policy terms. The last thing a business wants to hear after facing a crisis and successfully implementing its response plan is that coverage is denied because the work was performed internally or by "unapproved" vendors. The insurance policy should be fully aligned with your response plan and any other measures you are taking to protect the organization against cyber risks.

Most response plans call for at least some preliminary work to be performed by your internal team. You should proactively discuss this reality with the insurer during negotiations and request that at least some of those costs be covered—at least during an initial period that can serve as a bridge until an outside vendor can be brought in. This can be particularly important for technology companies that have confidential and propriety information that may be at risk unless internal safe-guards are implemented before a vendor accesses company systems and data.

Additionally, if the policyholder already has a trusted vendor that is familiar with (or may have even helped design) the response plan, the policyholder should raise that issue during the negotiation process and push for that vendor to be included on a preapproved list. A vendor's existing knowledge of the policyholder's systems and ability to respond immediately should ultimately prove beneficial for all concerned, including the insurance company. The policyholder may also be able to pre-select the law firm or firms listed in its cyber insurance policy as part of its team for defending third-party claims. Negotiating pre-approved billing codes and rates can help minimize disputes with the insurer down the road.