

The Metropolitan Corporate Counsel®

National Edition

www.metrocorpcounsel.com

Volume 23, No.1

© 2015 The Metropolitan Corporate Counsel, Inc.

January 2015

Insurance Coverage for Cyber Liability

Richard D. Milone
Genna S. Steinberg

KELLEY DRYE & WARREN LLP

Cybersecurity data breaches have increased dramatically over the last several years. These breaches impose significant costs on companies, including the costs of forensic analysis, credit monitoring, crisis management services, statutory fines, and – potentially – regulatory investigations and litigation. As recent high-profile data breaches have demonstrated, even a sophisticated company may be the victim of a cyberattack.

Insurance can play a vital role in a company's ability to mitigate the risks of cyber liability and manage its financial exposure. Unfortunately, however, insurance providers frequently deny policyholders' claims for cyber liability coverage under their standard commercial general liability (CGL) policies and are increasingly adding exclusions to their CGL policies to avoid such coverage. While the insurance indus-



**Richard D.
Milone**



**Genna S.
Steinberg**

***Insurance can play a vital
role in a company's abil-
ity to mitigate the risks of
cyber liability and manage
its financial exposure.***

try has begun to develop standalone cyber insurance policies that specifically address cyber liability, selecting and negotiating the right cyber insurance policy presents its own unique and significant challenges. Moreover, although insurers market these policies as an essential risk-management tool for any well-secured business, companies can still obtain significant coverage under their existing policies.

As the risk of cyber liability grows, it is important for companies to understand their existing coverage, weigh their coverage options, and seek experienced policyholders' insurance recovery counsel to negotiate policy terms and ensure that their contractual rights are fully enforced.

Coverage Under CGL Policies

CGL policies may provide significant coverage for cybersecurity data breaches. Among other things, these policies insure against damages arising from "personal and advertising injury," which is generally defined to include any "oral or written publication that violates a person's right of privacy." While some courts have denied

coverage for data breaches under CGL policies, holding that the "right to privacy" means simply the right to seclusion, other courts have upheld coverage, interpreting the "right to privacy" to include the right to keep private information from others.

Even in jurisdictions where courts uphold CGL coverage for cyber liability, however, insurers may assert a number of additional defenses. These defenses might include, for example, failure to comply with the insurance policy's notice provisions, failure to cooperate with the insurer, and failure to disclose the appropriate risks on the insurance application. Some insurers also argue that, at the time they drafted their policies, data breaches and other hacking activities were not prevalent, and that policyholders cannot claim coverage for risks that neither party contemplated at the time of drafting. Despite these obstacles, many policyholders have successfully secured cyber liability coverage under their CGL policies, through both settlement and litigation.

As courts have upheld coverage under CGL policies, however, the insurance industry has sought to eliminate cyber liability from its standard-form policies. The revised standard-form CGL policy – effective May 1, 2014 – explicitly excludes such coverage. Because the policy's language will generally control the coverage determination, a claim for cyber liability coverage under the revised standard-form CGL policy is probably futile. However, many insurance providers have not yet adopted the revised form and may be reluctant to do so. Insurers may fear that implementing the revised language will imply an admission that their existing policies provide cyber liability coverage. At the very least, adopting the revised form may imply that insurers' existing policies are ambiguous in this regard, thus warranting a construal of the policy in favor of coverage.

Thus, depending on the facts, allegations and policy terms, a CGL policy may remain

***Richard D. Milone** serves as Chair of Kelley Drye's Washington, D.C. Litigation Group and Co-Chair of its firmwide Insurance Recovery Group. Mr. Milone has successfully handled insurance recovery lawsuits in venues all over the country, particularly in Ohio, New York, Illinois, Virginia, California and Texas. During his 23-year career, he has tried matters to verdict before juries and arbitration tribunals, argued cases of first impression in state and federal appellate courts, negotiated complex, multi-party settlements and secured hundreds of millions of dollars in disputed insurance proceeds on behalf of policyholder clients. **Genna S. Steinberg** is an Associate in the firm's New York office. She focuses her practice on commercial and complex civil litigation, including disputes involving insurance, antitrust, trademark and patent matters, among others. She also works on domestic arbitration matters.*

Please email the authors at rmilone@kelleydrye.com or gsteinberg@kelleydrye.com with questions about this article.

a strong option for cyber liability coverage. Companies relying on their CGL policies for coverage should provide prompt notice to their insurers of any data breach allegations and hire experienced policyholders' insurance coverage counsel to evaluate and pursue their claims.

Coverage Under Specialized Cyber Liability Policies

Because of the challenges in obtaining cyber liability coverage under CGL policies, insurance providers have begun to develop specialized cyber liability policies. Insurers in both the U.S. and London markets are increasingly offering these policies under a variety of different names, including "cyber liability insurance," "privacy breach insurance" and "network security insurance."

Unlike CGL policies, cyber insurance policies are not standardized and vary widely among insurers. Nonetheless, these policies almost always cover both first- and third-party losses arising from cybersecurity breaches. First-party policies provide first-dollar coverage for losses to the policyholder's business. These policies cover lost revenue, breach notification costs and other crisis management expenses, such as forensic investigation, credit monitoring, call centers and public relations efforts. In contrast, third-party policies provide coverage for losses arising from the policyholder's liability to third parties, such as clients and governmental entities. These policies cover defense costs (including the costs of class actions, consumer demands, FTC investigations, and state attorney general proceedings) as well as the costs of any settlement or judgment against the policyholder.

Cyber insurance can be a relatively expensive investment, particularly for high-risk organizations that either generate most of their revenue online or store large amounts of data, such as online retailers, computer coding businesses, and healthcare institutions. Insurers who market these policies, however, contend that a well-tailored cybersecurity policy can significantly reduce the out-of-pocket expenses that

breached entities incur and that insurers allow recovery under these policies without dispute. Insurers also argue that obtaining cyber insurance actually reduces the risk of a cyberattack because insurers will either deny coverage or increase premium costs for companies that do not have adequate data security systems in place.

Given the lack of standardization and the competitive market for cyber insurance, the terms of cyber insurance policies tend to be highly negotiable. Before purchasing cyber insurance, a prospective policyholder is well-advised to consult with an experienced cyber liability coverage lawyer, who can negotiate key provisions in a way that maximizes coverage and minimizes disputes. There are a number of policy provisions to which prospective policyholders should pay particular attention:

Exclusions

As with CGL policies, cyber insurance policies may contain overly broad exclusions that defeat the intended purposes of the policy. Many policies, for example, exclude coverage for data breaches that the policyholder failed to take adequate precautionary measures to prevent. If drafted broadly enough, this type of provision could potentially exclude the type of negligent conduct that motivates companies to purchase cyber insurance in the first place. Cyber insurance policies also frequently exclude coverage for claims arising from contractual liability, statutory liability, unauthorized collection of data or acts of "foreign enemies." Prospective policyholders must negotiate with their insurers to narrow and clarify the scope of these exclusions.

Notice Provisions

Many cyber insurance policies contain overly onerous notice provisions, which may void coverage for the policyholders' negligent acts. Prospective policyholders must ensure that the notice requirements are not so broad or burdensome as to defeat the purpose of the policy itself.

Definitions: "Claim" and "Loss"

Cyber insurance policies must be drafted

broadly enough to protect the policyholder from the types of financial exposure that cyberattacks create. For example, a well-drafted policy should define "claim" to encompass non-traditional claims, such as FTC investigations, third-party subpoenas, and even verbal requests for information by government bodies. Similarly, the definition of "loss" should be broad enough to encompass the extensive crisis management services that companies must engage to mitigate the effects of a cyber breach, such as the costs of public relations efforts.

Alternative Dispute Resolution Clauses

Many cyber insurance policies contain alternative dispute resolution (ADR) clauses, which require policyholders to resolve coverage disputes through arbitration. Because of the private and confidential nature of arbitration proceedings, ADR provisions are generally in the policyholder's best interest. However, prospective policyholders must scrutinize these provisions to ensure that they are drafted fairly. Policyholders must ensure, for example, that the ADR provision does not require or allow for a biased arbitration panel comprised primarily of insurance industry executives. Moreover, there may be situations in which companies would prefer to proceed publicly, by initiating a lawsuit against the insurance carrier, and prospective policyholders should consult with counsel to determine whether it is appropriate to retain this option.

Conclusion

Insurance can play an important role in an organization's overall efforts to mitigate cyber risk. Given the prevalence of cybersecurity incidents, the insurance industry's evolving position on CGL policy coverage, and the emerging variety of insurance policies, companies are well-advised to understand their existing insurance coverage, carefully weigh their coverage options, and consult with experienced counsel who can assist in securing a policy that is properly tailored to the company's cyber-risk needs.