

PRESENTED AT

20th Annual Insurance Law Institute

November 12-13, 2015
Dallas, Texas

A Policyholder's Guide to Insurance Coverage For "Cyber" Events

Micah E. Skidmore

Micah E. Skidmore
Haynes and Boone, LLP
Dallas, Texas

micah.skidmore@haynesboone.com

214.651-5654

I. Introduction

The threats facing U.S. companies¹ from cyber attacks are myriad. Third-party claims by customers or employees for damages resulting from the disclosure of personally identifiable information or lack of access, loss of valuable trade secrets or other intellectual property of the insured or others, interruption of business operations, credit monitoring expense, damaged reputations, privacy notification, regulatory investigations, follow-on fiduciary and shareholder derivative litigation, and data loss are only a few of the risks to which businesses (and any other organization possessing material amounts of data) are exposed.² The financial stakes associated with any one of these risks are staggering.³

When it comes to insurance coverage, the potential “cyber” solutions now available in the market can seem equally vast and daunting. Within the past few years, most major insurance carriers have unveiled new or revised policy forms specifically designed to protect against the burgeoning threat of cyber attacks and related liability and other risks.⁴ While “liability” is invariably included in the titles of most “cyber,” “information security,” “network” or “privacy” forms, such policies also typically include what are traditionally thought of as first-party coverages from privacy notification coverage, crisis management, extortion, and vandalism coverage to data loss, business interruption, and extra expense. Still other policies may contain quasi-fidelity coverages protecting against loss resulting from computer fraud and funds transfer fraud. Even with respect to third-party liability risk, the terms and the resulting scope of coverage may vary widely from one policy form to the next. Alternatively, corporate insureds may address so-called “cyber” risks with customized “riders” and “endorsements” to traditional liability, property and fidelity policies.

With so many distinct choices for addressing such an important risk, it is critically important for corporate policyholders both to understand the potential issues that may arise from different “cyber” policy terms and select and negotiate the coverage that is most appropriate and most likely to avoid a dispute in the event of a claim. Part II of this paper lists key policy terms and the material considerations for each when negotiating dedicated “cyber” coverage.

¹ Hazel Glenn Beh, *Physical Losses in Cyberspace*, 8 CONN. INS. L.J. 55, 59 (2001) (indicating as early as 2001 that “90% of businesses have experienced computer security breaches, and losses to U.S. businesses in 1998 were estimated to have ‘exceeded \$200 billion.’” (citations omitted)); compare PONEMON INSTITUTE, IS YOUR COMPANY READY FOR A BIG DATA BREACH? 3 (Mar. 2013) (“76 percent of respondents say their organization already had or expect to have a material data breach that results in the loss of customers and business partners. Similarly, 75 percent say they have had or expect to have such an incident that results in negative public opinion.”).

² Cf. Robert H. Jerry, II & Michele L. Mekel, *Cybercoverage for Cyber-Risks: An Overview of Insurers’ Responses to the Perils of E-Commerce*, 8 CONN. INS. L.J. 7 (2001) (“[S]ome underwriters at Lloyd’s of London believe that ‘e-commerce will emerge as the single biggest insurance risk of the 21st century.’”).

³ PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 7 (May 2015) (“The US sample experienced the highest total average cost at more than \$6.53 million, followed by Germany at \$4.89 million.”).

⁴ See, e.g., ACE Privacy Protection Privacy & Network Liability Insurance Policy, Form No. PF-27000 (05/09); Beazley Information Security & Privacy Insurance with Electronic Media Liability Coverage, Form No. F00106 (052011 ed.); Cybersecurity by Chubb, Form No. 12-02-14874 (02/2009); Philadelphia Insurance Cyber Security Liability Coverage, Form No. PI-CYB-001 (05/10); Travelers CyberRisk Form No. CYB-3001 (Ed. 07-10); Zurich Security and Privacy Protection Policy, Form No. U-SPR-1000-B CW (7/09).

In the event that a policyholder elects to rely on traditional policies to address what is collectively identified with “cyber,” “network” and “information” security or “privacy” liability risks, it is equally important that the insured is familiar with the coverage issues and existing decisions addressing “cyber” claims under traditional first and third-party forms. Part III summarizes key coverage issues and decisions relating to “cyber” risks under traditional liability, property, and crime/fidelity policies.

II. What to Watch for When Purchasing & Negotiating Dedicated “Cyber” or Network/Privacy Coverage

Every “cyber” policy form is unique and deserving of a careful review. Nonetheless, among the variety of “cyber” insurance offerings available in the market, common issues arise. Here is a checklist to review when negotiating “cyber” coverage terms, including familiar policy provisions, pertinent considerations and related issues to avoid in anticipation of a claim.

Insuring Agreements

“Cyber” policy forms offered by many major carriers may include a litany of separate grants of coverage, including data loss, business interruption, privacy notification, credit monitoring, reputational response, cyber extortion, forensics and regulatory investigation response. When considering what policy form is appropriate, policyholders should carefully determine the risks to which their particular business operations are most susceptible and then attempt to match those risks with available insurance offerings. Whereas cyber extortion, for example, may be a significant concern for some businesses operating with a substantial public profile, the “reputational risk” associated with a cyber event for other online companies may be relatively small. Those insureds with a more narrow “cyber” risk profile might be better off selecting the form that is most specifically tailored to the risk at hand—if only to avoid the unnecessary premium associated with superfluous coverage. But as a general proposition, even for those policyholders with wide ranging exposure to a variety of different types of e-risks, a policy form with only a few, broad grants of coverage may be preferable to one with a dozen or more very narrow insuring clauses. All other things being equal, the form with the broadest single insuring clause may offer more protection and may be less susceptible to the argument (in opposition to coverage for a future claim) that, if the parties intended coverage, they would have expressly allowed for the risk at issue.

Who is Insured

When investigating a particular policy form, determine all elements of coverage that are tied to the definition of who is an “insured.” For example, most policies will require, at a minimum that a claim be made against an “insured.” Other policies will also limit covered “damages” to those that an “insured” incurs or is legally obligated to pay. Still other contracts limit covered “wrongful acts” to those committed by an “insured.” Particularly when the triggering conduct is tied to who qualifies as an “insured,” those individuals described in the definition of “insured” should include anyone within the insured organization responsible for network security, whether classified as employees or independent contractors. Alternatively, the “wrongful acts” that trigger coverage should be broadly stated to include conduct, not only by an “insured,” but also