Published on *The National Law Review* https://natlawreview.com

Top Tips and Traps for Cyber Insurance Buyers

Article By:

John G. Buchanan III

Marialuisa S. Gallozzi

Although the National Cybersecurity Awareness Month of October has come to a close, it is not too late for corporate counsel and risk managers to be thinking about cyber-risk insurance — an increasingly essential tool in the enterprise risk management toolkit. But a prospective policyholder purchasing cyber insurance for the first time may be hard put to understand what coverage the insurer is selling and whether that coverage is a proper fit for its own risk profile. With little standardization among cyber policies' wordings, confusing labels for their covered perils, and little interpretive guidance from case law to date, a cyber insurance buyer trying to evaluate a new proposed policy may hardly know where to focus first.

After pursuing coverage for historically major cyber breaches and analyzing scores of cyber insurance forms over the past 15 years, we suggest the following issues as a starting point for any cyber policy review:

- ***Push your limits.*** Although total cyber limits up to $500 million are reportedly available in the insurance marketplace, many major companies' cyber programs top out at much less. Our experience teaches that even limits of $100 million might fall far short of the total losses from an historically major data breach. **Tip:** If your company's principal concern is protection against catastrophic cyber exposures, then consider a higher self-insured retention and build the highest tower of limits above that retention that you can afford.

- ***Beware of sublimits*.** Many cyber policies cap particular kinds of loss at amounts less than the total policy limit. For example, some insurers sublimit coverage for regulatory and Payment Card Industry (PCI) expenses; in a claim for a major payment card breach, these sublimits can generate disputes over how various expenses are characterized and can complicate the timing and presentation of losses. **Tip:** Some primary insurers are willing to set full-policy limits for all or most of the coverage grants principally involved in a typical payment card breach. Negotiate as few sublimits as commercially feasible. **Trap:** Some endorsements purporting to cover ransomware are effectively exclusions masquerading as coverage grants with small sublimits. Ransomware already falls within the scope of "cyber extortion" coverage grants in many cyber forms; don't accept a ransomware-specific endorsement without reviewing both the policy and the endorsement carefully.

- ***Push back the Retro Date.*** Network intrusions are latent injuries: a hacker may be lurking on your system for months before you discover the breach. Most cyber policies exclude loss arising from events happening before a specified "retroactive date," regardless of when loss is discovered. **Tip:** The default setting for the retro date is the first inception date of cyber coverage, but some insurers are willing to set it up to a year earlier. Negotiate the earliest retro date you can.

- ***Get your cyber application right.*** Cyber-risk insurance applications typically consist of detailed and highly technical questionnaires, and many cyber policy forms expressly recite that statements in the application are incorporated by reference into the policy, material to the risk, and relied upon in issuing the policy. **Trap:** An insurer bent on denying a claim may pore through those questionnaires looking for misstatements that might provide a basis to void the policy. For example, the insurer's complaint in *Columbia Cas. v. Cottage Health* (C.D. Cal., filed May 31, 2016) alleged that misstatements in the "Risk Control Self Assessment" included in the insured's cyber insurance application provided grounds to rescind the policy. **Tip:** *Cottage Health* illustrates the importance of a careful application process. The company's legal department, with the assistance of outside counsel as needed, should play an active role in coordinating IT and risk management input into the cyber application, which requires expertise from both functions. A particular challenge in many cyber insurance applications is the disclosure of prior cyber incidents, with attendant privilege concerns.

- ***Mind the (coverage) gap, please.*** A policyholder must look across its entire insurance portfolio to consider whether significant gaps exist, and if so where. The connectedness of the Internet of Things is a prime example of the potential disconnectedness among common insurance programs. Most cyber policies exclude physical bodily injury and property damage, because traditionally conventional property and general liability policies covered such physical harms. **Trap:** Over the past decade cyber-related exclusions or restrictions have proliferated in standard property and liability policies. **Tip:** Major property insurers now commonly offer upgraded versions of their policies with cyber-related coverage extensions. More recently, specialty policies covering liability for "cyber-physical" losses have entered the marketplace. If the Internet of Things or networked Industrial Control Systems (ICS) play a part in your operations, explore both your current property and liability programs and these gap-filling alternatives carefully.

- ***And don't forget "other people's insurance."*** Your own cyber policy must fit into your larger ecosystem of risk management arrangements. Under typical vendor or service contracts, counter-parties may be required both to indemnify you for cyber-related losses and to procure cyber insurance, both for themselves and for your company as an additional insured (AI). **Tip:** Check the "other insurance" clause in your cyber policy to determine whose policy will apply first if you are an AI under another party's cyber policy. **Trap:** A certificate of insurance from a contracting party's broker is not the same thing as the policy itself. Especially with cyber policies, which vary widely in their terms, the certificate may not accurately state either the scope of the other party's coverage or your status under their policy. **Tip:** Implement internal risk management procedures, to request and promptly review the policies required under insurance procurement clauses in all contracts; to calendar those policies' renewal dates and identify any changes in coverage; and to notify the other party's insurer in the event of a cyber incident.

Of course, this list is not exhaustive. Other issues that bear scrutiny include the cyber policy's

treatment of defense and selection of defense counsel; its coverage for regulatory investigations and other government proceedings; exclusions that might purport to preclude coverage for employees' human error; contractual liability exclusions that may conflict with your indemnity or insurance obligations under contracts with third parties; and many more. But every policy review must begin somewhere. The half-dozen issues above will get most first-time purchasers started down the road to understanding what they are buying.

National Law Review, Volume VII, Number 307