



# Ways to Get Your Cyber Insurance Company to Pay Claims

By Joshua Gold and Vianny M. Pichardo

As companies incorporate ever-evolving technology, daily headlines show escalating cyber risks. Cyber risks can run the gamut, from personally identifiable information (PII) data breaches, to “internet of things” perils, to regulatory and class actions. Faced with these across-the-board cyber risks, businesses are looking toward their insurance policies to cover resulting losses. However, the current state of the cyber insurance market makes it difficult to navigate these risks and adequately protect companies from liability through reliable insurance coverage. A number of lawsuits and arbitrations have arisen involving cyber insurance companies disputing insurance coverage for cyber claims under cyber-specific insurance policies.

To help policyholders maximize the chance of an insurance recovery from cyber-related losses, below is our list of 10 cyber insurance recovery tips.

**1** Make sure your cyber insurance matches the way you conduct online business and host data. For example, if you use cloud computing or other vendors for hosting and processing data, make sure you have cyber-risk insurance policies that can be tailored to reflect that the policyholder may delegate to a third-party data management and hosting. Further, it may make sense to see if you can become an additional insured under the vendor’s insurance program to enhance the chances that insurance protection will be available.

**2** If you do business with individual consumers and obtain their PII, make sure you have coverage (including attorneys’ fee coverage) for the inevitable expenses of responding to informal inquiries and formal proceedings that ensue from state attorneys general, the FTC and potentially others when a breach occurs.

**3** Make sure that your cyber insurance covers breaches arising from mobile devices that may or may not be connected to the company’s computer network. More and more employees can access systems through tablets, smartphones, and PCs. The ever-growing capacity of hard drives and the ubiquity of portable drives mean that some employees may create security risks, even when the device is not logged into the company servers. This is especially true when sensitive data has not been properly encrypted.

**4** With the latest technological trend to “wire” all manner of gadgets, electronics, and transportation (the so-called internet of things), risks abound involving bodily injury, property damage and invasion of privacy. Such perils are usually covered under CGL policies. However, many policyholders are seeing

exclusions for cyber related claims in their CGL policies. Couple this reality with the fact that some cyber policies actually have exclusions for bodily injury and property damage claims, and businesses have a possible defect if the circumstances are just bad enough. Therefore, make sure to properly construct your insurance program, being mindful of not only cyber policy terms, but the terms of other insurance policies in the portfolio.



Underwriters will be focusing more and more on cyber risk areas, and insurance application responses often are used against policyholders to contest insurance claims.

**5** In light of recent cyber related derivative lawsuits against company directors and officers, D&O underwriters are focusing more and more on cyber risks. Making sure D&O insurance (primary, excess, Side A, etc.) responds to suits targeting company managers and directors can be done by removing any cyber-related exclusions or sublimits.

**6** Do not forget about business income coverage and reputational damage coverage in addition to class action privacy and securities litigation coverage. An increasing number of cyber attacks are launched without a profit motive, where the main intent is to paralyze a company's business operations. As such, cyber insurance coverage that pays time-element claims resulting from reputational damage and business interruptions is often important for a company that may attract the attention of hackers with a "cause."

**7** Complete insurance applications carefully, including D&O applications. Underwriters will be focusing more and more on cyber risk areas, and insurance application responses often are used against policyholders to contest insurance claims.

**8** Avoid cyber insurance policies with contractual liability exclusions. If your underwriters will not remove them, pick the policy terms that keep such exclusions as narrow as the market place affords. Unless you only do business with the general public, it is not uncommon to see contractual liability claims arise in conjunction with statutory claims, negligence claims and other forms of relief.

**9** If you are buying or renewing specialty cyber insurance policies, make sure you work with an experienced broker. While dedicated cyber insurance products are flooding the market, the marketplace is in flux, fragmented and confusing to navigate. Because there is presently a lot of competition in the cyber insurance marketplace, policyholders in many industries will find that an array of coverage terms are open for negotiation.

**10** Provide notice to your insurance companies promptly after a breach. Significant costs are incurred quickly once a breach is detected, and insurance companies particularly hate being handed bills before they have had notice of a claim. Providing relevant notices and advising of these costs promptly can increase the odds of recovering from your insurance companies without a wrestling match.



*Joshua Gold, Chair of Anderson Kill's Cyber Insurance Recovery Group, represents numerous corporate and non-profit policyholders in a broad range of industries in insurance coverage disputes. His practice involves matters ranging from data breaches to international arbitration, D&O, business income/property and commercial crime claims, and marine insurance.*



*Vianny M. Pichardo is an attorney in Anderson Kill's New York office. Vianny's practice concentrates in insurance recovery, exclusively on behalf of policyholders, in corporate and commercial litigation and environmental law.*

