Insurance for Data Breach and Other Cyber-Attacks: What Every Company Should Consider

Data breaches and other cyber-attacks have become part of our daily newscycle. Last week, a prominent health insurer disclosed that hackers had gained access to millions of patient and employee records. This is just the latest in a series of high-profile attacks, each one seemingly more brazen and stunning in scope. Of course, strong security systems and procedures are essential to defending against a breach. In addition, every company's toolkit for cybersecurity should include insurance to mitigate, if not eliminate, the losses resulting from cyber-attacks.

Businesses increasingly have turned to cyber liability insurance. These policies contain a "grab bag" of coverages, which may range from the immediate costs of responding to a data breach (for example, the costs of technical experts and public relations consultants); to the costs of notifying consumers or other affected groups; to the business interruption resulting from an attack; to follow-on litigation and regulatory proceedings. What some companies may not appreciate, however, is that cyber liability insurance is not their only recourse, and that they may well have coverage under other policies—policies that they obtain annually as part of their insurance program. It is therefore critical that every business assess what its insurance program provides, and augment its coverage if and as appropriate.

When purchasing or renewing a cyber liability policy, the company should carefully scrutinize its options. Cyber liability policies are not standard, and the offerings can vary considerably from one insurer to the next. Further, important aspects of the policies may be negotiable. For example, cyber liability policies may exclude claims arising from "terrorism." It is suspected that some of the recent, highly-publicized data breaches were instigated by foreign governments. If that is proven, then will insurers argue that the attacks constituted excluded acts of "terrorism," even though they bore none of the traits of conventional terrorist acts? An aggressive insurer may well seek to rely on the terrorism exclusion to deny coverage in this scenario. A savvy business will try to eliminate this issue before it could ever be raised, by seeking to remove any terrorism exclusion from its cyber liability policy upon purchasing or renewing coverage.

During the renewal process, it is also important to pay attention to

changes that insurers seek with respect to other policies. Commercial general liability (CGL) policies contain (an often-overlooked) coverage for certain conduct that "invades a person's right to privacy." Back in 2011, Sony suffered a data breach that resulted in many follow-on consumer class actions. Sony argued —correctly, in my view—that its CGL policies covered the costs of defending and settling the class actions. In response, one of Sony's insurers filed suit against Sony in New York, and several other insurers joined in. The insurers prevailed over Sony in the trial court, but Sony has filed an appeal. Simultaneously, during the 2014 renewal process for many companies, insurers have sought to modify the CGL coverage for invasions of privacy, by seeking to add language expressly excluding many types of claims arising from data breaches. This too may be negotiable, and insurer efforts to add the new language should be resisted.

A company should continually assess and reassess its insurance coverage as its business evolves and as cyber-threats become ever more sophisticated. In the event of a breach, the company should provide prompt notice to the relevant insurer(s), because substantially delaying notice may—depending on the circumstances—impair its rights to insurance coverage. Further, if and when lawsuits and regulatory proceedings are initiated, the company should consider providing separate notice (depending on the policy language), as the legal proceedings may implicate a separate or overlapping set of policies. Taking these steps will minimize the impact of a breach and maximize the company's entitlement to insurance coverage.

For more information, please contact:

Miles C. Holden, Partner
415-995-5039
mholden@hansonbridgett.com