Why Companies Should Consider Cyber Risk Coverage

By Natasha Lisman, Esq.
January 12, 2016

The SEC's Division of Corporation Finance has recently advised companies that they should regularly review the adequacy of their disclosures of the cybersecurity risks they face, including the descriptions of their insurance coverage for such risks. Cybersecurity breakdowns and the attendant data breaches range from a variety of deliberate and sophisticated digital attacks on computer systems to unintentional and rather mundane events such as the misplacement of physical tapes holding data.

The losses and expenses arising out of such incidents for which insurance coverage is needed include:

- the costs of complying with the federal, state and international requirements for post-data breach notifications;
- the costs of legal and forensic services as well as fines and penalties related to government investigations;
- the costs of crisis management and public relations services;
- the costs of defense and indemnity (for settlements or judgments) for claims of invasion of privacy, identity theft, misappropriation of intellectual property or confidential business information, and loss, corruption or theft of data;
- loss of use of computers and systems and the attendant business interruption;
- harm to reputation and goodwill.

All organizations – whether or not regulated by the SEC – that use computers to collect, maintain and retrieve data, would be wise to heed its guidance and assess the cybersecurity risks arising out of their business activities and the adequacy of their insurance coverage for those risks.

Cyber Risk Insurance Coverage

An organization's ideal risk management strategy is to obtain specific cyber risk insurance coverage under either a so-called cyber risk policy or cyber risk endorsement(s) to one or more of its existing traditional insurance policies, such as Commercial General Liability (CGL), Professional, Errors & Omissions (E&O), Directors & Officers (D&O), Employment Practices Liability (EPL) and property policies. Such cyber-risk policies or endorsements are not standard insurance products but, rather, are tailored to provide a variety of different types of coverage, often in modular format, for different risk profiles and requirements. This wide array of options offers freedom of choice and cost control, as well as challenges that call for sophisticated expert insurance advice.

This article originally published in ***InsideCounsel.com*** *and is reprinted with their permission.*

Cyber-insurance coverage has been available in the insurance market for more than 20 years. The products have greatly evolved and proliferated in recent years in response to the dramatic rise in data breaches and other cybersecurity incidents. But it is striking how often organizations, even sophisticated information technology giants, fail to include cyber-risk coverage in their insurance programs. When caught dealing with a cybersecurity incident without such coverage, they seek to find coverage under their traditional policies. The most common strategy is to invoke coverages for "personal and advertising injury" and "property damage" under CGL policies.

Fitting cybersecurity incidents into such coverages requires creative arguments, such as characterizing theft of data as "publication," the costs of complying with statutory data breach notification requirements as personal injury, exposure of data subjects to junk mail as invasion of privacy, and damage or corruption of data as property damage. As reported case law shows, insurers have met such claims with stiff resistance, arguing, in essence, that insureds are trying to fit the square pegs of their cyber risk losses and expenses into the round holes of traditional policies.

Problems with Inadequate Coverage

The result has been a proliferation of coverage disputes and litigation, with mixed results for the sides.[1] A notable and instructive example is the recent declaratory judgment litigation in New York state courts between Zurich American Insurance Corporation and Sony Corporation of America. It was initiated by Zurich when Sony, which did not have cyber liability insurance – demanded coverage under its CGL policies for the underlying lawsuits arising from the notorious incident of hackers gaining access and stealing massive amounts of personal identification and financial information of PlayStation users. The trial judge found that there was "publication" for purposes of the "personal and advertising injury" coverage but that the second prerequisite for such coverage – that "publication" be committed by the insured, i.e., Sony – was not met as the wrongful acts constituting "publication" were perpetrated by third parties, i.e., the hackers.

Sony took an appeal and its outcome was eagerly awaited in the business and insurance world as potentially providing significant precedent on the scope of coverage for data breaches and other cyber risks under traditional CGL policies. However, during the pendency of the appeal, after it was fully briefed and argued, the parties – as smart businesses often do when faced with the uncertainties of litigation – opted to resolve their dispute by mediation and settlement instead of a court judgment.

Whether or not the parties in the Sony case achieved settlement on their own or with the help of mediation is not known and appears to be covered by their confidentiality agreement. However, unsettled state of the applicable law and, hence, high unpredictability of the results of all-out litigation or arbitration – as is the case with insurance coverage for cyber risks – are precisely the conditions under which mediation with a neutral with relevant expertise is an ideally suitable method of dispute resolution. ●

Natasha Lisman is a JAMS neutral, based in Boston. She specializes in insurance and reinsurance disputes. She can be reached at nlisman@jamsadr.com.

[1] For a veritably encyclopedic overview of arguments pro and con of cyber risk coverage under traditional business insurance policies and the related case law, see R. D. Anderson, ***"Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz,"*** 49 Tort Trial & Ins. Prac. L. J. 529, Winter, 2014; and for an up-to-date overview, "Coverage in the Age of Data Breaches," a PowerPoint presentation at the October 8, 2015 Massachusetts Reinsurance Bar Association Symposium, available at **http://mreba.org/symposium2015.php**. Click **here** to download our Presentation.

This article originally published in ***InsideCounsel.com*** *and is reprinted with their permission.*