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

Cybersecurity Insurance Fills Important Gaps in Liability Insurance Coverage

Article By:

Jeffrey S. Raskin

The twenty-first century challenges posed by data breaches and cyber crimes do not fit neatly into the space occupied by traditional liability insurance policies. As a result, courts have had a difficult time grappling with data breach claims under such policies, which highlights the need for companies to consider cybersecurity liability insurance coverage as a more targeted option to cover against losses incurred by cyber crimes and data breaches.

Below, we outline a company's potential need for cybersecurity liability, as well as discussing certain coverage options and considerations. In the coming weeks, we will continue to discuss these issues as they relate to "first-party" insurance, which can be purchased to cover losses to an insured's property, data, and business that result from a data breach.

Traditional liability insurance policies cover the insured against its legal liability to pay damages because of injury to "tangible" property (such as land and buildings) and/or due to an invasion of the right to privacy (such as the publication of private information). Data breaches, however, present unusual circumstances and consequences for which traditional insurance policies—and traditional interpretations of such policies—are not well-equipped. Tens of millions of consumers can be affected by a single data breach, which can lurk unsuspected for years and originate from anywhere in the world.

Some courts have imposed limits on the scope of general liability insurance coverage in connection with data breaches. In one case, the insured incurred millions of dollars in "response costs" (e.g., paying for identify theft services) after computer tapes containing employment-related data for thousands of employees were lost. The court held that the insurance claim was not covered under the insured's traditional liability insurance policy because the insured had not been sued for damages by any of the employees and because there had been no "publication" of the information stored on the tapes that resulted in a violation of any person's right to privacy. In another case, a trial court held that the acts of third-party hackers were not covered because the policy at issue only covered injuries stemming from the publication of non-public data by the insured itself, not outside hackers.

On top of this, the insurance industry is increasingly adding exclusions to liability insurance policies that eliminate coverage for certain types of data breach claims, or eliminate such coverage

altogether. Consequently, companies should not assume that they will be protected against data breach claims under traditional liability insurance policies. The safer, more reasonable assumption is that data breach claims will not be covered under the terms of a traditional policy, or that any available coverage will be severely limited.

To fill the gaps in data breach/cyber crime protection that exist in traditional insurance policies, dedicated data breach and cyber risk coverage is available in either standalone policies or as an "add on" to a company's existing policy. Of course, data breach/cyber risk coverage is still fairly new and untested. Numerous products are available, each with different terms, conditions, definitions, and coverage afforded by the various insurers. However, there is still little in the way of guiding authority from the courts with respect to how the coverage applies (or does not apply) in the "real world."

In the liability ("third-party") insurance context, dedicated data breach policies can be written specifically to cover a company against a whole host of losses that may not be covered under its traditional liability insurance policy, including the following:

- Claims against the insured for invasion of privacy resulting from the publication and disclosure of confidential data by anyone, not just the insured
- Claims resulting from the loss of third-party data, regardless of whether the data was "published" or disclosed to the public
- Claims resulting from the failure to anticipate or prevent the transmission of a virus to third parties
- Legal and forensic expenses incurred when responding to governmental inquiries that follow a data breach
- Costs incurred in the process of notifying consumers, employees, and others potentially injured by a data breach
- Crisis management and public relations expenses incurred to address negative publicity arising from a data breach
- Costs incurred in consumer or employee credit monitoring, identity theft services, and fraud monitoring services following a data breach

The relatively non-standardized nature of dedicated data breach liability insurance coverage presents a significant opportunity for companies to design such coverage with the company's particular risks in mind, and to negotiate favorable contract terms and conditions. Specific issues for insureds to consider include the geographical territory covered by the policy (since cyber attacks can originate from anywhere in the world) and the potentially "retroactive" nature of the policy (since network intrusions and data leaks can continue undetected for quite some time before being discovered).

National Law Review, Volume V, Number 285