BURR FORMAN LLP

Are You Covered?—A Basic Primer on Cyber Insurance Offerings

Articles / Publications
07.02.2021

The digitization of various products, services, and business processes over recent years has been a boon for business. But, as our clients are well aware by now, it has brought attendant cybersecurity risks. The recent spate of ransomware attacks on organizations like Colonial Pipeline (disrupting nearly half of the East Coast's gas supply for days) and JBS (affecting nearly 20% of the country's meat market) underscores this reality. Of course, companies face a number of other cyber risks, from computer-based "social engineering" schemes to "cryptojacking," where a company's computing systems are furtively hijacked to mine crypto currency.

Each company faces unique cyber risks based on the nature of their business, the state of their systems, and a host of other factors. It is vital that companies of any size take stock of their risks and consider whether their insurance policies cover any cyber perils they are most likely to face. Increasingly, traditional liability insurance and first-party insurance (*e.g.*, crime or commercial policy) offerings purport to exclude any loss or damage caused by cyber-related incidents. A recent ISO Commercial Policy endorsement titled "Cyber Incident Exclusion," for instance, states that the insurer "will not pay for loss or damage caused directly or indirectly" by a "Cyber Incident," "regardless of any other cause or event that contributes concurrently or in any sequence to the loss." (ISO Form No. CP 10 76 12 20). The form endorsement defines "Cyber Incident" as:

- Unauthorized access to or use of any computer system (including electronic data).

RELATED PROFESSIONALS

Robert S. Given

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Are You Covered?—A Basic Primer on Cyber Insurance Offerings

- Malicious code, virus or any other harmful code that is directed at, enacted upon or introduced into any computer system (including electronic data) and is designed to access, alter, corrupt, damage, delete, destroy, disrupt, encrypt, exploit, use or prevent or restrict access to or the use of any part of any computer system (including electronic data) or otherwise disrupt its normal functioning or operation.
- Denial of service attack which disrupts, prevents or restricts access to or use of any computer system, or otherwise disrupts its normal functioning or operation.

Id.

In response to the escalating cyber threats insureds face, insurers now offer stand-alone cyber insurance policies. These policies vary considerably in their scope of coverage, but a considerable number of policies currently offered cover both liability and first-party losses arising out of a hack or data breach. Below is a snapshot of the types of cyber coverages that all insureds should consider when evaluating their current or future cyber insurance policies. Some policies may title or refer to the coverages below using different language, but what follows is a generalized description of key coverage provisions.

Event Management: Covers your costs to manage the event itself, including:

- Attorney Fees
- Forensic Investigation Costs
- Costs of compliance with statutory or contractual breach notification requirements
- Post-breach public relations management

Business Interruption: Covers lost income (typically in the form of reduced gross earnings) arising from cyber-related business disruptions.

Destroyed Digital Asset Restoration: Covering the costs of data retrieval and system restoration.

Extortion: Covers your costs to pay to resolve ransomware, denial of service attacks, etc.

Regulatory Investigations; Fines & Penalties: Covers costs incurred by imposition of breach-related penalties or investigations.

Network Interruption: Covers the loss of revenue/ extra expense you incur because your network's down.

Third-Party Security/Privacy Liability: Covers your liability to third-parties arising out of the loss or compromise of their data. *E.g.*:

- Someone manipulates your network to breach someone else's network through an API connection you have.
- You fail to protect customer or vendor information (SSN, cc, medical info, passwords) due to a cyber attack.

Are You Covered?—A Basic Primer on Cyber Insurance Offerings

Media Liability: covers defamation, invasion of privacy, copyright infringement, and other losses arising out hazards like unauthorized social media posts or advertisements.

In addition, to maximize coverage or account for unique cyber risks, insureds may be able to take advantage of certain emerging or specialized endorsements on offer by some carriers. These include coverage for so-called "bricking," where a cyber attack somehow physically damages your hardware and renders it irreparable; "cryptojacking" (discussed above); "cyber criminal reward expenses" (paying rewards for information that leads to the identification or arrest of a cybercriminal); and "invoice manipulation losses."

It is critical that organizations of all types and sizes take a careful inventory of their current insurance coverages and maximize their potential for coverage in the event of a cyber incident. A reputable broker along with an attorney with significant experience in the cyber insurance realm will be a helpful resource in making decisions as to which coverages to purchase and maintain.