Shumaker

JANUARY 21, 2026 | PUBLICATION

"Avoiding the Dreaded Denial: What Corporate Policyholders Should Know About Their Cyber Insurance Policies"

Navigating a cyber claim with your insurance carrier can be a daunting task especially when a potential denial is looming. Before getting to "no," corporate policyholders should familiarize themselves with potential pitfalls and common exclusions that can operate to preclude coverage.

INDUSTRY SECTOR

Technology

SERVICE LINE

Corporate, Tax & Transactions
Insurance Recovery
Litigation & Disputes
Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Meagan R. Cyrus

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Cyber insurance policies can be written on an occurrence or claims-made basis. Claims-made policies respond to claims that are first made within the policy period, even if the alleged acts took place prior to the effective date of the policy. Conversely, occurrence-based policies provide coverage solely for events taking place during the policy period but may be reported at any time during or after the policy period. These types of policies can be complicated enough. Misunderstandings regarding their coverages and exclusions are compounded by the fact that cyber insurance policies are largely written on a manuscript basis, unlike traditional insurance products which are more standardized and heavily regulated by state departments of insurance.

It is crucial to understand your risks and what you are purchasing to guard against those risks. Starting with the initial building blocks, comprehensive cyber insurance typically provides two types of coverages: first-party (*e.g.*, loss of revenue due to a cyber-attack; extortion fees; data recovery support) and third-party (*e.g.*, lawsuits from third-parties affected by a breach; credit monitoring for affected customers).

Exclusions

Some common exclusions to look out for include:

- Government-issued fines – governmental agencies may penalize a policyholder for failure to secure consumer data, delaying notification of a breach, or failing to implement applicable security measures.
- Breaches involving employees or independent contractors-while not as common, employee or independent contractor dishonesty can lead to a claim.

- Terrorism or war – attacks increasingly involve state actors, which insurers may attempt to classify as an act of war or terrorism.
- Related or prior acts – insurance is designed to cover fortuitous events. Therefore, knowledge of events that took place prior to the policy's inception can operate to exclude coverage. The language regarding how the prior acts are characterized can be crucial.

Negotiation for particular endorsement coverages overriding these exclusions can be discussed on the front-end of obtaining coverage, to the extent it is economically feasible for your level of risk.

Terms and Conditions

Your policy is subject to a host of terms and conditions as part of the insuring agreement. The duty of cooperation is essential in the event of a claim. Policyholders are generally required to share relevant information at the request of the insurer. However, policyholders are under no circumstances required to respond to irrelevant, burdensome requests for information. Working with a qualified broker and insurance counsel can assist in making this important distinction.

Insureds are under an obligation to provide prompt notice of claim. As a breach can at times be difficult to detect and may fall under the radar for a period of time, be cognizant of the timing requirements under the policy and ensure they are in accordance with your expectations.

Applications

As is the case with many coverage forms, and as part of the application process, underwriters often ask insureds to disclose any prior events that may give rise to a potential claim, which they will then explicitly exclude from coverage. Insureds will want to be mindful of how these events are described to the carrier given the severe implications. Also, you should ensure you understand whose knowledge will apply to bar coverage and the knowledge standard applied.

Cyber insurance applications will also ask detailed questions regarding the policyholder's confidential information held, security systems, employee training, and processes for avoiding and detecting a breach. The party responsible for answering these questions should involve those with specific knowledge such as IT professionals when necessary.

Crucial information needed to assess cyber liability risk is collected in the insurance application, which becomes part of the terms of coverage and false statements in the application could lead to recission of the policy entirely.

Please contact Meagan Cyrus or a member of Shumaker's Insurance Recovery Team with questions or for more information.

Shumaker