Lowenstein Sandler

Insurance Recovery

March 31, 2020

What Actions Should Companies Take to Secure Cyber Insurance Coverage for Losses Related to Cyber Incidents in the COVID-19 Landscape?

By Michael D. Lichtenstein and Jason D. Meyers

As companies scramble to respond to the COVID-19 pandemic, one area that may not, but should, be on their radar is the terms and coverage provided by their cyber insurance policies. Certainly COVID-19 is not a computer virus, but it has drastically affected businesses' reliance on technology to keep operating. With increased dependence, though, comes increased vulnerability. What's more, cybercriminals view crises as opportunities and ruthlessly exploit human and technological weaknesses. Therefore, companies now should reassess the coverage their cyber policies provide (particularly if the policy is up for renewal soon) and be prepared to respond in the event of a cyber incident.

Though specific cyber insurance policies vary widely, generally a cyber policy provides some of the following coverage for expenses and losses related to security/privacy/cyber events:

- Breach responses
- Business interruption (i.e., lost profits due to your company's computer or network failure)
- Cybercrime (e.g., funds transfer and social engineering fraud)
- Data and systems restoration
- Dependent business interruption (i.e., lost profits due to your supplier's or customer's computer or network failure)
- Extortion
- Media liability claims (e.g., libel, slander, defamation, and copyright infringement claims)
- Payment card breaches
- Privacy breaches
- Regulatory fines and penalties
- Technology services and products claims

First, companies should review the language of their cyber policies carefully. Does your policy adequately cover your company's risks? Do the terms of your cyber policy adequately include your company's computer and network systems? Are the total limits and sublimits of liability sufficient? What exclusions apply?

If a company's cyber policy is up for renewal, remember that not all policies are created equal and specific endorsements can be negotiated with insurers to best suit your company's needs. On a related point, if your company receives a nonrenewal notice, you must immediately begin to evaluate other renewal options.

Second, companies should continue to educate and train their constituents regarding best cyber practices.

Third, in order to maximize the potential for coverage under cyber policies, companies should take the following steps if or when a security, privacy, or cyber event occurs:

1. Provide timely notice. Though providing timely notice may seem obvious, it is essential for policyholders to do so since the policy's coverage may be broader than a policyholder intuitively understands and since many cyber policies are claims-made policies, which means that providing timely notice, even simply of circumstances, can secure coverage under the policy even after it expires if those circumstances later give rise to a covered claim. This is particularly important now as the insurance industry is preparing COVID-19-specific endorsements to drastically limit or eliminate coverage in new or renewed policies.

2. Seek counsel from a coverage attorney, especially if your insurer denies a claim. Insurers often initially deny claims. An experienced coverage attorney can advise you regarding your cyber policy and the factual and legal settings and, if possible, help you obtain the coverage your company purchased. For example, many courts interpret ambiguous policy language in favor of the policyholder, and certain jurisdictions are more favorable for securing coverage than others. Further, even if an exclusion in the policy applies, many courts interpret exclusions narrowly, and there are often exclusions to the exclusions.

Though many companies are rightly focused on the coverage provided by their first-party property (including business interruption), general liability, director and officer liability, employment practices liability, and other liability policies in the ever-changing landscape created by the COVID-19 pandemic, it is also critical for companies to review and understand their cyber policies. A greater reliance on computer systems and telecommuting to keep companies operational means a greater risk of cyber events that will result in loss.

To see our prior alerts and other material related to the pandemic, please visit the Coronavirus/ COVID-19: Facts, Insights & Resources page of our website by clicking here.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MICHAEL D. LICHTENSTEIN
Partner
T: 973.597.2408
mlichtenstein@lowenstein.com

JASON D. MEYERS
Associate
T: 973.597.2310
jmeyers@lowenstein.com