Lowenstein Sandler's In the Know Series

Video 2 -
Coverage Considerations for Ransomware & Cyber Attacks

By Eric Jesse
APRIL 2022

Eric Jesse: Hi, I'm Eric Jesse, partner in Lowenstein Sandler's Insurance Recovery Group. Welcome to “In The Know.”

Businesses continue to experience an unprecedented level of ransomware and cyberattacks, and insurance companies only expect those cyberattacks to increase as a result of Russia's recent invasion of Ukraine and the harsh economic sanctions that Western nations have imposed on Russia in response. Policyholders need to be prepared to navigate a difficult and hardening cyber insurance market as insurance companies reel from past claims experience, and as they anticipate future claims activity as a result of Russia's invasion. So what can policyholders do to prepare?

First, during this upcoming renewal, policyholders should pay careful attention to the war and/ or terrorism exclusions in cyber insurance policies. Not only will Russia's invasion of Ukraine cause insurance companies to take a much closer look at these exclusions, but a recent New Jersey court decision will as well. In that decision, the New Jersey court ruled that a war exclusion did not bar coverage for a cyberattack that originated out of Russia. The court held that the war exclusion only applied to physical, not cyber, warfare. So as insurance companies reevaluate the wording of their war and/or terrorism exclusions, policyholders need to make sure that those revisions do not operate in a way where the exclusion swallows up any coverage that would otherwise be available for cyberattacks that originate from Russia. Policyholders can do this by making sure that the exclusion has key and necessary carve- outs for cyber terrorism or cyberattacks, as will be defined in the policy, and to make sure that there are exceptions for key coverages, such as ransomware or business interruption.

Second, I don't need a crystal ball to tell you that when your cyber policy comes up for renewal, you will likely experience increased premiums again, increased retentions, lower supplements for key coverages such as ransomware, and more restrictive terms and conditions. Policyholders should work with their broker to start the renewal process earlier than they usually would, so that these issues are identified sooner. This will enable you to raise your concerns with your broker and your coverage counsel earlier in the process, and will also allow your broker if necessary to go out to the insurance market to obtain competing quotes from other carriers. And another reason to start the renewal process sooner rather than later is because policy holders should expect a much more intensive underwriting process. The days of just filling out a written application and submitting it to

the insurance companies are likely in the rear view mirror. Today, insurance companies expect comprehensive submissions with detailed information about cyber security protections that are in place training for personnel and contingency planning in the event of a cyberattack. And on top of that, cyber insurers may even want to interview your IT personnel, which is something that your company should take very seriously and fully prepare for.

We hope these tips will help you navigate the wild west of cyber insurance. Thank you for joining us, and we look forward to seeing you next month on “In the Know.”