Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ransomware Case Signifies Shift In Cyber Insurers' Stance

By **Lynda Bennett and Michael Scales** (November 12, 2021, 4:21 PM EST)

Lynda Bennett

Michael Scales

Ransomware attacks are on the rise. Lax security measures, which have become more acute in the work-from-home environment, continue to be exploited. Companies' systems are hacked into, their data is encrypted, and they face multimillion-dollar ransoms.

When faced with the chaos of a potentially devastating ransomware attack, businesses turn to their cyber insurers for immediate guidance and relief to help get their systems back up and running.

In the past, insurers routinely provided assistance and worked hand in hand with policyholders to cover losses and minimize damages from an attack.

However, due to the increasing size and frequency of these attacks, cyber insurers have recently adopted a more adversarial response to ransomware claims and are increasing premiums, skyrocketing self-insured retentions, narrowing policy terms and, more recently, advancing coverage defenses to avoid claim payments.

The parties' pleadings in a U.S. District Court for the Central District of California case that just recently settled illustrates how insurers are starting to change their attitudes toward these kinds of claims.

In Boardriders Inc. v. Great American Insurance Co.,[1] Boardriders — the parent company to apparel brands Billabong and Quiksilver — sought coverage under its cyber policy following a 2019 ransomware attack in which hackers shut down the company's networks worldwide and demanded nearly $25 million for the decryption keys.

The policy provided coverage for extortion and for business interruption losses resulting from the necessary interruption of business caused directly and solely by the extortion.

Boardriders contended that although it immediately tendered the claim to its insurer and expected immediate assistance, the insurer engaged in delay tactics by demanding detailed information, taking eight months to issue a coverage position.

It alleged that the insurer's representatives stated they were unable to confirm coverage at the time the claim was tendered, and instead required Boardriders to maintain a detailed summary of its costs.

Left without the cyber extortion coverage it expected to have readily available, Boardriders opted to try to restore its data from backups rather than pay the ransom out of its own pocket, and incurred significant losses during the months it was locked out of its systems.

Boardriders alleged that the insurer did not respond to its communications about its remedial plan of action, and instead made continuous and duplicative requests for information — much of which was compromised because of the ransomware attack itself — to engage in inappropriate delay tactics with the end goal of avoiding claim payment.

Boardriders contended that, in addition to requiring it to shoulder all of the burden and expense of attempting to restore its systems, and the losses resulting from downed networks, the insurer had also tried improperly to squeeze Boardriders' business interruption losses into a two-day window, despite the policy's promise to pay losses incurred over a 120-day restoration period.

Boardriders filed suit, alleging the insurer unreasonably delayed its coverage determination, improperly withheld the coverage benefits afforded by the policy and engaged in bad faith by cutting Boardriders loose when it needed insurance protection the most, i.e., in the wake of the ransomware attack.

Though the insurer eventually did make payments totaling about $5.6 million, it took the remarkable position in its counterclaim that it never owed that coverage, and sought to recoup most of it by arguing that Boardriders failed to prove that its claimed losses were caused by the ransomware attack.

The insurer also took issue with the documentation Boardriders submitted in support of its damages and claimed Boardriders failed to provide sufficient responses to its various requests for information.

Though the case settled last month,[2] and the court will not render decisions on these issues, the dispute that materialized between the parties is interesting to reflect upon for a number of reasons.

First, it signifies a shift away from the response that most policyholders have received in the immediate aftermath of breaches and extortion demands in the past several years, where the insurer partners with the policyholder to negotiate the demands and get systems back up as soon as possible.

The enormity and frequency of ransomware attacks has led insurers to start taking more entrenched positions on these claims and, on more recent renewals, to start placing sublimits on the amount of coverage provided for the cyber claims with the highest risk factors.

This is true even where the cyber policyholder is an insurer.

For example, CNA Financial Corp. recently disclosed in a U.S. Securities and Exchange Commission filing that it anticipates potential disputes with its own cyber insurers over coverage for a $40 million ransom it paid to hackers during a March ransomware attack.

Moreover, on more recent renewals, insurers are starting to place sublimits on the amount of coverage provided for the highest risk factor cyber claims.

To date, there has been little case law interpreting the terms of dedicated cyber policies because those claims have largely been paid.

The Boardriders dispute could foretell similar disputes between policyholders and their cyber insurers that could similarly lead to litigation. It will be interesting to watch how courts are going to react to insurers that do not pay on claims that are supposed to be covered by this niche insurance product.

Second, some of the grounds for the insurer's refusal to pay in Boardriders reflect a sign of the times and may portend changing policy language on cyber coverage forms.

The insurer here relied on language that limits business interruption coverage to those losses caused directly and solely by the cyber incident, and argued that outside factors, such as the COVID-19 pandemic and catastrophic weather events, contributed to the claimed losses.

The insurer even sought to claw back the nearly $5.6 million in payments it previously made to Boardriders, claiming it specifically reserved the right to do so.

This will likely become a hot issue in future cyber coverage disputes. Policyholders can expect insurers to make initial payments under a policy as a sign of good faith, and then later try to claw back those payments by raising similar causation arguments if their policies contain the same limiting language as the Boardriders policy.

Therefore, policyholders will be well advised to engage forensic accountants to help prepare their losses in a manner that is carefully documented and aligns with the coverage provided under the policy.

Policyholders should also keep careful eyes on their renewal quotations, as cyber insurers may look to narrow their coverage obligations by engrafting similar policy language on their forms.

Third, this case serves as an important reminder that policyholders should take care to keep insurers informed from day one after a breach has occurred, and to take all reasonable steps to fully document their claimed losses.

Here, the insurer alleged that Boardriders failed to provide an adequate description of the ransomware attack by providing few details about when the attack occurred and the nature of the ransom demand, and that Boardriders failed to respond to the insurer's requests for information.

Though Boardriders' complaint alleged a completely different story, this dispute nevertheless highlights the importance of putting insurers on immediate notice of the breach, keeping them informed about vendor engagement, and looping them in on forensic investigations, remedial action plans and government regulatory response plans.

Doing so will take another common coverage defense among insurers — lack of consent — off the table.

In sum, the dispute that arose between the parties in this case marks a shift in how insurers are handling cyber claims.

While they previously worked hand in hand with policyholders and routinely paid claims, they are now starting to transition into a tighter mode of handling claims and placing greater burdens on policyholders from the outset, ultimately forcing policyholders to deal with devastating ransomware attacks on their own, despite the hefty premiums policyholders have paid to secure insurance protection for these very scenarios.

The insurer's actions and coverage arguments in this case may reflect a broader shift in the

insurance industry at large, and policyholders should be on the lookout for insurers to take similar positions in future coverage disputes.

Lynda A. Bennett is a partner and Michael J. Scales is an associate at Lowenstein Sandler LLP.

[1] Boardriders, Inc. v. Great American Insurance Company (C.D. Cal., Docket Number 8:21-cv-1260).

[2] The related case, Great American Insurance Company v. National Union Fire Insurance Company of Pittsburgh PA and AIG Europe SA, No. 2:21- cv-06945-JLS-JDE, has also settled.
