FINE PRINT

3 Cyber Claim Insurance Coverage Lessons Learned in 2021

by Joshua Gold

With a cyber specialty insurance product market that is changing rapidly, becoming tighter, more expensive and more selective, key revelations from cases decided in 2021 are of particular relevance to policyholders looking to secure their insurance protection in the wake of a cyber incident.

Policyholders currently face what may be the toughest cyber insurance marketplace ever. Premium increases have been astronomical for many, and getting the same quality of protection is becoming more elusive—even for those organizations that have strong safeguards in place.

Despite this, it is not all doom and gloom. Decisions involving cyber claims under non-cyber specific insurance products have been largely favorable to policyholders throughout the year, reminding all that insurance coverage may be found across product lines in the wake of a multi-faceted cyber loss. Below are a few key takeaways from seminal coverage rulings during the year.

Lesson One is that the whole "silent cyber" narrative has to be taken with a grain of salt. A slew of commercial insurance policies (whether D&O, E&O, general liability/CGL, crime insurance, property insurance, etc.) may provide significant coverage for policyholder losses or claims, at least in substantial part.

For example, in the *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.* case decided earlier this year by the Indiana Supreme Court, the fact that the policyholder had refrained from purchasing a specific cyber coverage endorsement did not negate coverage under commercial crime insurance for a cyber loss resulting from a ransomware attack. The Indiana Supreme Court rejected the argument that a crime coverage insuring agreement could not cover the policyholder where it had failed to purchase specialized cyber coverage under a business package policy. Instead, the court expressly ruled that coverage had to be determined based upon the actual insuring language before it—not based upon external concepts such as what other insurance options might be sold in the market place.

Lesson Two is the need for evidence to support an insurance claim. In *G&G Oil*, the Indiana Supreme Court did not grant summary judgment to G&G because it was unable to determine whether the policyholder was in fact entitled to insurance coverage given the limited evidence presented. Instead, the court sent the case back to the trial court for further factual determinations as to whether the policyholder was tricked into letting the ransomware into its computing environment. The remand underscores the importance for policyholders to secure sufficient technological details surrounding the cyber incident and consequential harm to the policyholder.

Conversely, in a decision from an appellate court in Ohio issued just last month (*EMOI Services, LLC v. Owners Ins. Co.*), the court rejected the insurance company's motion to dismiss the case on grounds that the policyholder had not demonstrated direct physical loss (i.e., damage to its software) caused by a ransomware attack. The court found that deposition testimony from the policyholder's software developer and IT manager asserting that the attack damaged the company's software and data was sufficient to allow the coverage suit to proceed.

The bottom line is that after a cyber incident, for a host of reasons

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

December 2021

including coverage claim support, the organization is well-advised to secure detailed technological information concerning the attack, including the manner of entry, the systems and data targeted, the resulting harm, the duration of that harm, and any lingering damage caused by the incident. Computer forensic reports are also useful for addressing inquiries from regulators and law enforcement in the wake of security incidents.

Lesson Three stems from the *EMOI* court's rejection of the frequent insurance company assertion that cyberattacks on computer systems do not entail "physical loss or damage" to "covered property." The *EMOI* court rejected, among other arguments, the assertion that covered property only includes "tangible property," noting that for the purposes of the property coverage before it, the alleged requirement that the property be "tangible" was nowhere to be found. Indeed, the court rejected efforts to label media and other electronic items as uncovered property, relying in part on the 2020 decision in Maryland in *National Ink and Stitch v. State Auto Property and Cas. Ins. Co.* The *EMOI* court and the *National Ink* court rejected arguments that property insurance did not cover system damage caused by ransomware attacks when adverse computing issues lingered after attempted decryption of the affected files. The Ohio court concluded that "the policy contemplated that EMOI's software and reproduction of data was capable of being physical damaged, and [the IT manager] has testified that is was."

The decisions above indicate that policyholders should not discount the fact that their crime, property and other insurance products may cover cyber claims in whole or in part. While dedicated cyber insurance remains a very important insurance product to protect against cyber losses, it is not the only insurance product that can provide coverage. Further evidence of this came in 2021 when the Fifth Circuit Court of Appeals found coverage for cyber related claims under D&O insurance and CGL insurance for theft of customer funds and theft of payment card information respectively. Therefore, organizations need to make sure to consider notice and claim submission to all relevant insurance policies at the time a cyber incident occurs. R

Joshua Gold is a shareholder in Anderson Kill's New York office, chair of Anderson Kill's cyber insurance recovery group and co-chair of the firm's marine cargo industry group. He is co-author with Daniel J. Healy of Cyber Insurance Claims, Case Law, and Risk Management, forthcoming from the Practicing Law Institute.

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

December 2021