CYBER INSURANCE ALERT

MARCH 11, 2026

Help When Cyber Sub-Limits Are Improperly Applied

By Joshua Gold

Two Federal Court Decisions Reject Cyber Insurance Companies' Sub-Limit Claim Arguments

Two recent federal court rulings underscore the importance of questioning the increasing use of "sub-limits" to slash policyholder cyber protection.

More and more cyber insurance companies are trying to stuff claims into "sub-limited" coverage clauses rather than paying under the full policy limits otherwise promised. These sub-limit clauses can be included in policies for a variety of different perils including theft losses, ransomware payments, and non-hacking events. But policyholders need to confirm their coverage rights before yielding to such arguments about the supposedly "limited" nature of the protection. As demonstrated in two recent cases, insurance companies may be improperly applying sub-limits in an effort to evade the full protection of the cyber coverage promised.

On February 24, the U.S. District Court for the Northern District of Texas ruled in **Cici Enterprises LP v. HSB Specialty Insurance Co.** that the cyber insurance company was improperly applying a sublimit to greatly reduce payments for its policyholder's malware loss.

The policyholder CiCi suffered a malware attack, encrypting its systems. Data was also stolen. The cyber insurance policy covered, among other things, "Cyber Extortion" up to $3 million.

The cyber policy also provided a $250,000 sub-limit of coverage for something defined as a "Ransomware Event," which purported to include any related Information Privacy Event, a related Network Security Event, and a related System Disruption. Overall, the policy contained seven Insuring Agreements for claims and loss from Information Privacy Liability; Network Security; Business Interruption; Cyber Extortion; Financial Fraud; Media Content; and Reputational Harm.

The clause below purported to define how sub-limits would be applied:
B. SUB-LIMITS OF INSURANCE

The cyber insurance company argued that its maximum payout for the malware claim was $250,000 rather than the $3 million promised for cyber extortion.

© 2026 Anderson Kill, P.C.

The policyholder argued against application of the sub-limit, and the federal court agreed "that CiCi's interpretation of the Ransomware Sub-Limit Endorsement is supported by the Policy language and structure, that is, that the Endorsement is not applicable on its face to Insuring Agreement D. Cyber Extortion."

Notably, the court found that "notwithstanding HSB's contentions that the 'Policy's intent is glaringly obvious' and 'clearly states that the Endorsement applies to all insuring agreements[,]' the Endorsement lacks any explicit language specifying that it applies to all the Section I Insuring Agreements. Instead, the Ransomware Sub-Limit Endorsement states that it is 'added to section II. Limits of Insurance' without making any reference to modifying Section I. Insuring Agreements. Section II. Limits of Insurance, however, does not afford any coverage to CiCi, but merely establishes HSB's maximum liability 'with respect to the Insuring Agreement to which each such Sub-Limit of Insurance applies….'" The court further reasoned that the "Ransomware Sub-Limit Endorsement does not state that it modifies or alters coverage under Insuring Agreement D. Cyber Extortion."

The court also noted that the Ransomware Sub-Limit Endorsement "does not even include the words 'Cyber Extortion,' or 'Extortion Loss' related to 'Cyber Extortion.' Instead, it states that '[a]ll other terms, conditions, and exclusions of the Policy shall remain unchanged.'"

The court also heeded the legal maxim that if words of limitation are to be applied to cut off coverage, the language must be express and clear: "If HSB wanted the $250,000 sub-limit to apply across the board, regardless of the Insuring Agreement, then it was incumbent upon HSB to expressly and clearly state that. Having not done so, it cannot now complain."

And perhaps most importantly, the court also ruled:

- the structure of the definition of 'Cyber Event' reinforces that, under the Policy, these two terms are distinct and separate types of events. 'Ransomware Event' was added as a type of 'Cyber Event' and joined the other types of 'Cyber Event,' including Information Privacy Event, Network Security Event, and Extortion Threat. Based on the amended definition of 'Cyber Event,' by its plain language, the court determines that the inclusion of 'Ransomware Event' was meant to be treated as a separate event from the other types of 'Cyber Event,' including being separate and distinct from an 'Extortion Threat.' As the drafter of the Endorsement, if HSB intended for 'Ransomware Event' as merely a subset of an 'Extortion Threat,' then it could have made that intent clear by stating so.

The court also permitted CiCi's claims of Texas Insurance Code violations to proceed, finding that

- CiCi has provided sufficient evidence to raise a genuine dispute of material fact from which a reasonable jury could find that HSB violated Chapter 541 of the Texas Insurance Code, notwithstanding that the parties dispute the application of the Endorsement. Specifically, CiCi has provided evidence that 'HSB's actions and that of its managing general agent, At-Bay, rise to the level of bad faith due to misrepresentations and failures to disclose information to CiCi that was critical to the coverage CiCi sought and was afforded under the Cyber Insurance Policy.'

Analogous 2025 Decision from the Second Circuit on Sub-limits for Computer System Outage Loss

The decision in CiCi follows on the heels of a pro-coverage ruling in the Second Circuit Court of Appeals rendered last September—also involving the application of a sub-limit for a computer system outage.

© 2026 Anderson Kill, P.C.

In ***Ariz. Beverages USA, LLC v. Hanover Ins. Co.***, no. 23-1177 (2d Cir.), the policyholder suffered a system outage causing loss of historical financial data. The power surge also prevented the policyholder from accessing "its computer systems to see account balances, receivables, inventory, and order information." The policyholder sought coverage under its property policy, including for audit expenses. This in turn led to the bank demanding regular audits in order to keep the credit facility in place. The policy had promised "Equipment Breakdown Coverage" which included protection for "Extra Expense". The property policy also covered "Data Restoration," under a sub-limit, which the policy defined as the "necessary cost to research, replace[,] and restore lost 'data.'"

The insurance company argued that it did not have to cover the increased accounting costs for the audit, as the sub-limited data restoration coverage was exhausted and the extra expense coverage was inapplicable. In a Summary Order dated September 2, 2025, the Second Circuit ruled that the policyholder was entitled to coverage for the audit expenses related to the loss of certain financial information that jeopardized a credit facility with its bank. Similar to the CiCi decision, the panel decided that the insurance company's argument was not supported by the plain language of the Extra Expense clause because the "provision does not tie the end of the restoration period to the repair, replacement, or rebuilding of 'covered equipment.'"

The panel also rejected the argument that the audit expenses could only be covered by the specific sub-limited clause of the property policy rather than a more general insuring agreement of the same insurance policy. Here, the insurance company argued that "the policy's inclusion of bespoke provisions covering data loss demonstrates that the restoration period cannot be tied to Deloitte's efforts to recreate Arizona's lost financial data."

The Second Circuit rejected this argument, finding:

- But nothing in the plain language of the policy provides that the Data Restoration provision is the exclusive vehicle for policyholders to seek recovery for damages associated with lost data. And to the extent that the policy's inclusion of specific terms addressing data loss introduces ambiguity into whether the Extra Expense provision covers the cost of replacing Arizona's 2017 financial data, New York law requires us to interpret "any ambiguities . . . against the insurer and in favor of the insured."

Conclusion

The bottom line is that policyholders should take insurance company arguments over the application of sub-limits with a big grain of salt. As the cyber insurance claim process has become more adversarial in recent times, disputes continue to arise with aggressive arguments over multi-million dollar losses somehow being covered not under the broad coverage of the main insuring agreements, but instead "subject to" a sub-limit in a fractional amount. The above cases decided by federal courts this year and last should help policyholders to push back.

© 2026 Anderson Kill, P.C.

Authors

Joshua Gold is a shareholder in Anderson Kill's New York office and serves as chair of the Cyber Insurance Recovery Group and co-chair of the Marine Cargo Insurance Group.

ANDERSON KILL

Known as the Policyholder Powerhouse™, Anderson Kill is a pioneer in insurance coverage litigation: we have more experience in litigating, trying and settling insurance coverage disputes than any other law firm. As the only four-time winner of Business Insurance's Legal Team of the Year (including 2024), our firm has an extraordinary record of obtaining insurance coverage for policyholders in connection with all manner of insured losses. The firm has offices in New York, NY; Boston, MA; Los Angeles, CA; Newark, NJ; Philadelphia, PA; Stamford, CT; and Washington, D.C.

© 2026 Anderson Kill, P.C.