LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What We Know From Early Cyberinsurance Rulings

By **Peter Halprin and Rebecca Schwarz** (September 3, 2024, 3:32 PM EDT)

Peter Halprin

Rebecca Schwarz

Concerns about cyber risk continue to be atop lists of what keeps general counsel, risk management professionals and C-suite executives up at night.

And these concerns are well-founded. Three major incidents have occurred this year: the Change Healthcare cyberattack in February, primarily **affecting** healthcare;[1] the CDK Global **cyberattack** in June, primarily affecting car dealerships;[2] and the Crowdstrike outage in July, affecting a broad range of businesses including airlines, airports, public transit, healthcare and financial services.[3]

What these incidents share in common is that the business interruptions that companies face can be due to their connections with other businesses that are directly affected — even if they themselves were not an intended target. To address these contingent liabilities, the recent incidents have also raised the profile of contingent business interruption coverage, coverage for the very types of losses that many businesses have suffered as a result of these attacks.

While a variety of cyberinsurance products have come to market, and continue to evolve, to reduce the financial impact of such risks, there had been very little litigation interpreting cyberinsurance coverage.

Given this, recent cyberinsurance decisions therefore provide some much-needed context and nuance to our understanding of cyberinsurance, and the manner in which it protects business income losses. In this article, we will delve into these decisions and their implications for policyholders.

Clarity on Coverage Grants, Causation, and the Period of Restoration

In three seminal decisions — Southwest Airlines v. Liberty Insurance Underwriters Inc., **decided** by the U.S. Court of Appeals for the Fifth Circuit in January, New England Systems Inc. v. Citizens Insurance Company of America, **decided** in the U.S. District Court for the District of Connecticut in December 2022; and Fishbowl Solutions Inc. v. Hanover Insurance Co., **decided** in the U.S. District Court in the District of Minnesota in November 2022 — courts have interpreted key coverage phrases to explain how coverage grants and causation work in the cyberinsurance context.[4]

Likewise, in Arizona Beverages USA LLC v. Hanover Insurance Co., **decided** in the U.S. District Court for the Eastern District of New York in July 2023, and Heritage Co. Inc. v. Hudson Excess Insurance Co., **decided** by the U.S. District Court for the Eastern District of Arkansas this May, courts interpreted the "period of restoration" in the cyberinsurance context.[5] Each case will be discussed in turn.

Coverage Grants and Causation: Southwest Airlines

Southwest is a seminal ruling regarding coverage for business income losses under cyberinsurance, with the Fifth Circuit having to confront the scope of the phrase "solely as a result of" when measuring business income losses.

As the Fifth Circuit explained in Southwest Airlines, the general purpose of business interruption

insurance is "to compensate an insured for losses stemming from an interruption of normal business operations ... thus preserving the continuity of the insured's business earnings by placing the insured in the position that it would have occupied if there had been no interruption."[6]

Likewise, as with any other contract, "the general duty to mitigate damages may come into play as a factor."[7]

For background, the Southwest dispute began with a system failure affecting approximately 475,839 customers. Following the disruption, Southwest incurred various costs to mitigate its damages. When seeking coverage, Southwest included in its losses these mitigation efforts, including the costs of FareSaver promo codes, travel vouchers, refunds, Rapid Rewards Points (redeemable for airline tickets for members of its frequent flyer program), and advertising costs (to extend a sale Southwest was conducting at the time of the system failure) for a total of $77 million in losses.[8]

After Southwest collected $50 million from its tower of cyberinsurance coverage, the next carrier up denied Southwest's claim, arguing that Southwest's covered losses did not exceed $50 million as its losses were not solely as a result of the system failure, but instead costs Southwest decided to incur for customer-related rewards programs, practices and promotions.

The Fifth Circuit rejected the insurer's attempts to avoid such costs, remanding the case to the lower court and noting that the insurer would have to explain why these costs do not constitute covered mitigation expenses.[9]

In light of Southwest, policyholders can take some comfort in the notion that mitigation activities undertaken as a result of an incident should be covered.

Coverage Grants and Causation: New England Systems

In another case assessing whether an insurer was obligated to reimburse business interruption losses sustained due to a data breach, the court considered the extent to which an insured's business had to be impaired for there to be coverage for business interruption losses.

In June 2019, New England Systems experienced a data breach affecting it and several of its clients.[10] As a managed service provider whose operations include "restoring backups, fixing servers, performing virus scans on machines, installing software patches, assisting with emails, addressing malware, helping clients recover from ransomware attacks, and helping clients recover from viruses," it decided to remediate the issues caused by the breach on its own without bringing in a third party because they believed it would be more efficient.[11]

In handling the remediation internally, the company had to turn down work for certain clients with which it had service agreements, which ultimately resulted in those clients not renewing their service agreements.

The insurer refused to cover the managed service provider's business interruption losses, arguing it suffered no disruption to its business activities and no loss of income as a result of the data breach. In support of this argument, the insurer pointed to an increase in total income when compared to the prior year.[12] In response, the company was able to point to deposition testimony from former clients who cited the data breach as their reason for not renewing their service agreements.

The court rejected the insurer's argument, finding that the "[p]laintiff does not need to demonstrate that it was completely unable to perform its typical business activities to claim the coverage it seeks" and "it is enough that Plaintiff was unable to function at full capacity."[13]

The court also found "that the term 'actual impairment' in the Policy is broad enough to include the forced reallocation of resources from a covered data breach, from services Plaintiff planned to provide to clients, on one hand, to efforts Plaintiff took to remediate the effects the data breach had on its clients, on the other."[14]

Based on the reasoning in New England, policyholders can take some comfort in the notion that losses should be covered even after a partial return to service if the policyholder remains unable to function at full capacity.

Coverage Grants and Causation: Fishbowl

In another case considering business interruption losses under a cyber policy, a court had to confront whether losses resulted from a cyber incident. The court in Fishbowl, like the Fifth Circuit in Southwest and the court in New England, found that losses resulting from a cyber incident were covered.

In November 2019, a bad actor hacked into a Fishbowl employee's email account and set up rules such that emails regarding invoices and payments were forwarded to a separate account.[15] As background, Fishbowl, a technical consulting and software development company, would generate and send invoices for the work it performed over email.[16] The bad actor thus used its control over invoices sent by Fishbowl for work performed to third parties to direct payments to the wrong bank accounts.[17]

The insurer argued that there had been no loss of business income because "business operations" only refers to income-generating activities, and invoicing clients did not generate income for Fishbowl.[18] The court rejected this argument, looking to the language of the policy and the types of data breaches covered to determine that "business operations" was not constrained to income-generating activities.[19]

The insurer also argued that the damages were not a direct result of the data breach because the loss would not have occurred but for a third-party's negligence and breach of contract in paying the invoice to the wrong account.[20] However, like the court in Southwest, the court in Fishbowl found that since the loss would not have occurred without the bad actor, the losses were "directly resulting from" the data breach.[21]

Measuring the Period of Restoration: Arizona Beverages and Heritage Co.

Picking up where Fishbowl left off, the Eastern District of New York relied on the conclusions in Fishbowl to find that audit expenses were part of the insured's usual business operations and thus qualified as "Extra Expenses" under the policy.[22]

In that case, Arizona Beverages suffered a power surge at its corporate headquarters resulting in a catastrophic failure of its account operating system.[23] The insured was able to repair the hardware and restore the backup data by January 2018, but backup data from 2016 and 2017 needed for an annual audit was permanently destroyed.[24] The insured worked with its auditor on revised procedures that cost hundreds of thousands of dollars and took until October 2018.[25]

In Arizona, the court also rejected the insurer's argument that the restoration period ended when the hardware was restored in January 2018, noting that the restoration period continued until the property was "rebuilt, repaired or replaced" or when "business is resumed at a permanent new location."[26]

Reasoning that audit data proved unrecoverable and the updated audit procedures were a reasonable way to repair, replace or rebuild the lost data, the court found that the restoration period continued until the audit was completed and that the audit expenses themselves were covered.[27]

In contrast to the decisions in Southwest Airlines, New England, Fishbowl, and Arizona, the Arkansas District Court in Heritage took a narrower view of the definition of "business income losses" while still emphasizing that the purpose of coverage is meant to put the insured in the same position it would have been in if not for the loss.

Heritage experienced a ransomware attack that disrupted its business for months with the exact duration of the interruption period in dispute. Pursuant to Heritage's policy, "Business Income Loss" included "net profit before income taxes that the Insured is preventing from earning during the Interruption Period;" and "[n]ormal operating expenses incurred by the Insured (including payroll), but solely to the extent that such operating expenses must continue during the Interruption Period and would have been incurred had there been no interruption or degradation of service" with additional amendments by endorsement.[27]

The policy further explained that business income loss shall mean "[f]or manufacturing operations, the net sales value of production less the cost of all raw stock, materials and supplies used in such production."[28]

In seeking coverage under the policy, Heritage argued that its business income losses should be calculated using the method provided for manufacturing operations, arguing even though it was not a manufacturing company, "manufacturing operations" was simply meant as an illustrative example.[29]

However, the court rejected Heritage's argument, finding that "[t]he correct methodology to determine Heritage's covered business income loss is to subtract from covered 'normal operating expenses' those that Heritage was able to pay from revenue it received during the Interruption Period."[30]

In reaching this conclusion, the court reasoned that the policy "is also designed to prevent the insured from being placed in a better position than if no loss or interruption of the business had occurred."[31]

Takeaways

1. Given the potential financial implications of cyberattacks and other cyber risk, companies should consider the bottom-line protection provided by cyberinsurance, including broad business interruption coverage that extends to contingent liabilities and losses.

2. In cyber coverage grants, "as a result of" and "directly resulting from" should be read broadly to include any losses that would not have been incurred but for the cyber incident even if there were intervening causes.

3. Business income and business operations can include losses associated with non-revenue generating activities.

4. Restoration periods should be construed broadly as initial system restoration may not mean that a business is back to preloss operations.

Peter A. Halprin is a partner and Rebecca Schwarz is an associate at Haynes and Boone LLP.

[1] https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

[2] https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html.

[3] https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

[4] Southwest Airlines v. Liberty Insurance Underwriters Inc., 90 F.4th 847 (5th Cir. 2024), New England Systems, Inc. v. Citizens Insurance Company of America, 3:30-CV-01743, 2022 WL 17585966 (D. Ct. Dec. 12, 2022), and Fishbowl Solutions, Inc. v. Hanover Insurance Co., No. 0:2021cv00794, 2022 WL 16699749 (D. Minn. Nov. 3, 2022).

[5] Arizona Beverages USA LLC v. Hanover Insurance Co., No. 20-1537, 2023 WL 4564872 (E.D.N.Y. July 17, 2023) and Heritage Co. Inc. v. Hudson Excess Insurance Co., No. 4:22-cv-82-JM (E.D. Ark. May 22, 2024).

[6] Southwest, 90 F.4th at 853.

[7] Id. at 854.

[8] Cite.

[9] Id.

[10] New England, 2022 WL 17585966 at *1-3.

[11] Id. at *1, 3.

[12] Id. at *5.

[13] Id. at *8.

[14] Id.

[15] Fishbowl, 2022 WL 16699749 at *1.

[16] Id.

[17] Id. at *2.

[18] Id. at *4.

[19] Id. at *6-7.

[20] Id. at *7.

[21] Id. at *8.

[22] Arizona, 2023 WL 4564872 at *4.

[23] Id. at *1.

[24] Id. at *1-2.

[25] Id.

[26] Id. at *5.

[27] Id. at *5-6.

[28] Heritage at *2.

[29] Id.

[30] Id. at 5.

[31] Id. at 6.

[32] Id.