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

Cos. Seeking Cyber Coverage Can Look To Key Policy Terms

By **Christine Montenegro, Brian Choi and Léa Dartevelle Erhel** (March 18, 2024, 4:12 PM EDT)


Christine Montenegro


Brian Choi


Lea Dartevelle Erhel

A few weeks ago, a cyberattack on the UnitedHealth Group reportedly paralyzed two services in charge of processing electronic payments and medical claims.

The incident illustrates the mass disruption that hackers can have on a business, often with reverberating effects on its customers, vendors and partners.

For the past decade, cyber crime has posed a serious, if not existential, threat to every company with a digital presence. The specter of a disruptive cyberattack will only grow over time — both in frequency and sophistication — as cyber criminals diversify their arsenal of weapons through the use of new technologies, including artificial intelligence.

And the losses will be staggering. By some accounts, the costs associated with global cyber crime are expected to reach $10.5 trillion in 2025, up nearly three-fold from $3 trillion in 2015.[1] But it will not just be the behemoth corporations that bear these losses — if anything, smaller companies will likely absorb a significant share, especially if their investments in cybersecurity lag behind those of their larger and better-resourced counterparts.

But not all cyberattacks are created equal, and the damage they inflict can materialize in different ways, resulting in a wide array of losses where coverage, depending on an insured's type of cyber policy, is not readily apparent.

In the most obvious example, a cyberattack can completely shut down a business. In the more likely scenario, however, a cyberattack can occur through clandestine means by paralyzing some, but not all, of the company's capabilities. It can cut off an insured's ability to communicate with customers or vendors, or to collect on a specific revenue stream.

Thus, while the company may be able to function — or at least maintain the appearance of functioning — without knowing that it has been attacked, it certainly is not running its business in the ordinary course.

As the business environment becomes more fraught with cyber risk, companies should be aware of the expanded interpretations of several key policy terms that mean they may recover under cyber business interruption policies or other coverage — even if their business hasn't completely shut down.

Cyber Business Interruption Policies

In the face of a cyberattack, an insured may believe that it can only recover under the sublimits of a cyber policy — such as provisions concerning the ransom payment, fraudulent transfer of funds or the issuance of fraudulent invoices to customers. While these provisions may offer relief in the typical scenario involving third-party criminal conduct, the coverage is often capped at an amount well below the actual loss.

An insured should therefore consider whether its policy offers business interruption coverage — where higher limits of loss would apply, sometimes by millions of dollars more — even in cases where the cyberattack did not fully shut down their business.

Indeed, given the context-specific nature of business interruption losses, courts have increasingly recognized that cyber policies should be interpreted flexibly, and have endorsed coverage for losses short of a complete cessation of the business.

It is therefore no surprise that business interruption claims have emerged as a significant cost driver for 57% of cyberinsurance claims in the past five years — a number that may only increase as companies seek coverage for losses resulting from various forms of interruption to their business.[2]

For example, consider a consumer goods company that uses a payment processing platform that is hacked by cyber criminals. The cyber criminals can replace the company's bank account information — which the payment processor uses to settle all revenue derived from the company's sales to the company — with unauthorized third-party account information.

The payment processor may then unwittingly settle a substantial amount of the company's revenue to the third-party accounts before the company realizes that its account has been compromised. Would the loss of such funds constitute a loss under a business interruption policy?

An insurer might opine that coverage does not exist because the hack did not actually shut down the company's ability to conduct business. In other words, an insurer might point out that while the insured was deprived of receiving some revenue, it could nevertheless continue selling its goods to consumers.

But the answer to whether business interruption coverage exists is more nuanced and lies in the plain language of the policy. The typical business interruption clause in a cyber policy provides coverage for "an actual interruption of the insured company's business operations caused by" a cybersecurity breach.

In recent years, with cyber losses mounting at exorbitant levels, insureds have taken a more aggressive posture on claiming business interruption loss, with an increasing focus on broadening the interpretation of terms like "business operation" and "interruption."

Expanded Meaning of "Business Operations"

To determine whether a policy covers a business interruption in a cyber-incident, the insured should evaluate what it means for its business to operate in the normal course.

As an initial matter, according to the Law Dictionary, the plain meaning of "business operations" is the "ongoing recurring activities involved in the running of a business for the purpose of producing value for

the stakeholders."[3]

Based on that definition, a company could argue that its business operations cover the routine collection of online revenue — a recurring activity that is vital to running the company's business. In other words, a business interruption does not necessarily mean a complete shutdown of operations.

Courts have also begun to agree.

In 2022, the U.S. District Court for the District of Minnesota held that a business interruption loss can result from the mere loss of a company's ability to communicate with its customers.

In Fishbowl Solutions Inc. v. Hanover Insurance Co., the court construed the term "business operation" expansively — rejecting the insurer's view that its definition should be limited to "usual and regular business activities" like "income-generating business activities" — and holding that it covered "all business activities performed with a certain frequency and consistency."[4]

According to the court in Fishbowl, the insured's business operations suffered an interruption when, as a result of the cyberattack, the insured "could not reliably, at all times, communicate and send invoices" to its clients.

One month later, in New England Systems Inc. v. Citizens Insurance Co. of America, the U.S. District Court for the District of Connecticut agreed with Fishbowl's rationale, expanding the scope of covered "regular business activities" to include certain "client services" that the insured could not perform while it sought to remediate the consequences of a data breach.[5]

And again, in July 2023, the U.S. District Court for the Eastern District of New York followed suit in its ruling in Arizona Beverages USA LLC v. Hanover Insurance Co. that an insured's ability to conduct its annual audit fell squarely within its usual "business operations" which it defined as "activities undertaken on a regular basis that are essential to the company's continued existence."[6]

Expanded Meaning of "Interruption"

It is important for insureds to construe the term "interruption" expansively as well, particularly where the policy does not expressly define such a term.

The court in New England Systems noted that "interruption" does not necessarily mean the total suspension or cessation of a business; it can mean something less, where a "policy holder may be compensated for lost income, regardless of whether the business continued to operate at a reduced level immediately following the covered loss."[7]

And the court in Fishbowl appears to have treated the term "interruption" and "impairment" co-extensively, holding that the "ordinary meaning of impairment is an inability to function at full capacity," and that such a term "is sufficiently broad to encompass the impact here of a bad actor's interference with [the company employee's] email" and ability to communicate with customers.

First-Party Policies

First-party policies for property or commercial general liability may also provide coverage for a cyberattack that partially interrupts a business. To qualify for coverage under property and CGL policies,

insureds must offer proof of "physical damage" to "tangible property."

In recent years, in examining whether the property damage insuring clause requirements have been satisfied, courts have interpreted the term "damage" to encompass "loss of use," "loss of reliability," or "impaired functionality" to use or access, computer data. Thus, if a cyberattack deprives the insured from utilizing its computer data, even temporarily, then the losses attributable to the inability to use such data may be covered under a property policy.

For instance, in National Ink & Stitch LLC v. State Auto Property & Casualty Insurance Co., the U.S. District Court for the District of Maryland held in 2020 that lost data and the compromised operability of a computer system resulting from a ransomware attack qualified as "direct physical loss" under a business property insurance policy.

In doing so, the court rejected the insurer's position that "physical loss or damage" meant the "utter inability to function," and found that the replacement of a functioning but slowed down computer system was covered.[8]

Similarly, in Eyeblaster Inc.v. Federal Insurance Co., the U.S. Court of Appeals for the Eighth Circuit held in 2010 that spyware causing crashes and poor computer performance triggered coverage under the "loss of use" definition of the policy, despite the fact that the computer remained operational.[9]

Key Takeaways

A company should carefully examine its cyber policy to determine which sub-limit or insuring clause covers the full scope of the cyber loss. While provisions for "funds transfer fraud" or "fraudulent payment instruction" may offer relief, the coverage is often capped at a limit well below the actual loss.

A "business interruption" provision, on the other hand, has a greater limit — sometimes by millions of dollars depending on the type of loss — and may potentially offer a way to recoup most, if not all, of the loss.

In the cyber context, business interruption can take many forms. The question of whether the cyberattack "interrupted" the insured's "business operations" is context-dependent, and subject to an expansive interpretation that can be favorable to the insured. An interruption to business operations can range from a company's loss of revenue to its temporary inability to communicate effectively with its customers and vendors.

A company should thoroughly take stock of all its insurance policies. It is possible that noncyber policies for first-party property or commercial liability offer an option to recover the expenses to repair, replace or otherwise remediate damaged technology.

For many of these policies, the company must demonstrate physical loss or damage to property. In cyber cases, this may mean ensuring that the policy does not explicitly exclude computer systems as covered property, and determining whether the company has suffered a "loss of use" of its systems and hardware as a result of the cyberattack.

Christine A. Montenegro and Brian S. Choi are partners, and Léa Dartevelle Erhel is special counsel, at Kasowitz Benson Torres LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/.

[2] https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html.

[3] https://thelawdictionary.org/business-operation/.

[4] 2022 WL 16699749, at *3, 6, 9 (D. Minn. Nov. 3, 2022).

[5] New England Sys., Inc. v. Citizens Ins. Co. of Am., No. 20-cv-1743, 2022 WL 17585966, at *8 (D. Conn. Dec. 12, 2022).

[6] Arizona Beverages USA, LLC v. Hanover Ins. Co., No. CV201537GRBLGD, 2023 WL 4564872, at *4 (E.D.N.Y. July 17, 2023).

[7] See also Maher v. Cont'l Cas. Co., 76 F.3d 535, 539 n.1 (4th Cir. 1996); Icue Corp. v. U.S. Fid. & Guar. Co., No. 07-cv-1781, slip op. at 2 n. 1 (E.D. Pa. Apr. 23, 2008) ("[T]he term 'necessary suspension' should not be construed to require a total cessation of business operations as a prerequisite to payment.").

[8] 435 F. Supp. 3d 679, 686 (D. Md. 2020).

[9] Eyeblaster, Inc. v. Federal Ins. Co., 613 F.3d 797 (8th Cir. 2010) (applying Minnesota law).