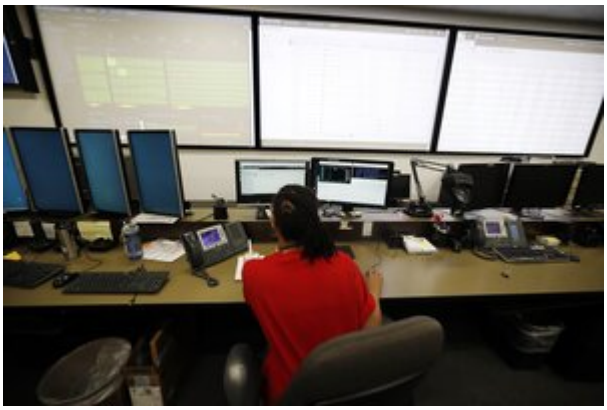
LAW360

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

Ohio Ransomware Ruling Heightens 'Silent Cyber' Worries

By **Daphne Zhang**

Law360 (November 29, 2021, 9:05 PM EST) -- An Ohio appeals court's recent split ruling in a ransomware case shocked insurance attorneys, with some saying the decision contradicts hundreds of recent COVID-19 coverage decisions and could pin so-called silent cyberinsurance risks on unsuspecting insurers.



Insurance attorneys said an Ohio appeals court's split ruling was a slap in the face after hundreds of recent rulings in COVID-19 insurance coverage disputes came to the opposite conclusion on property damage. (AP Photo/David Zalubowski)

In the ruling, a three-judge panel of Ohio's Second Appellate District found that a company that lost access to its system after hackers held it for ransom had potentially experienced property damage that could be covered by its property insurance policy.

Lawyers say that finding raises questions about the very nature of what constitutes a loss or damage in standard property insurance contracts, and could expose insurers to modern cyber risks they did not account for.

Insurer attorneys told Law360 that the Ohio decision flies in the face of the spate of **recent COVID-19 coverage rulings** because the majority said that property policies do not require "tangible damage," and that loss of use and access of a property can be covered.

Property insurance addresses physical items like a company's computer server instead of software and data on that server, insurer attorneys say. Most COVID-19 insurance decisions show that a property has to be tangibly changed to be covered and that businesses' temporary loss of access, such as those caused by government closure orders or cyberattacks, is not covered, they say.

Tangible damage also plays a role in the ongoing battle over what's known as silent cyberinsurance — when a regular property or general liability policy is applied to cyber risks. The fight among insurers and policyholders is only becoming more fierce as standalone cyber premiums skyrocket and cut policy limits amid increasing cyberattacks, according to industry observers.

The appellate panel majority said a medical billing company — Electronic Medical Office Integration Services — **could potentially get coverage** from Owners Insurance Co. after hackers encrypted its software and demanded a ransom. The opinion penned by Judge Chris Epley said that EMOI's

temporary loss of access to its system could constitute property damage. The panel also refused to toss the bad faith claim, saying Owners should have consulted an IT specialist when denying EMOI's claim.

The decision was somewhat fractured, with Judge Mary E. Donovan concurring in the majority ruling and Judge Michael L. Tucker dissenting. In his dissent, Judge Tucker found that Owners had made the correct coverage decision, so it couldn't have done anything in bad faith.

According to court records, EMOI's policy covers physical loss or damage to "media." The billing company has maintained that both its computer server and its software are covered media, while Owners argued that only the physical computer server — on which the software is stored — is covered.

Michael S. Savett, a partner at Clark & Fox who represents insurers, said he believes the majority felt sorry for EMOI's experience and was trying to find coverage for it. But the policyholder only paid $162 for $10,000 in media coverage, he pointed out. Owners carved out a separate cyber coverage but did not charge the right amount, he added.

"When underwriting for property and liability policies, insurance companies do not typically look at a company's security systems or evaluate the strengths and weaknesses of their network, because underwriting for that type of risk falls within the cyberinsurance arena," he said.

Judith Selby, a partner at Kennedys CMK, said the Ohio majority's opinion is "torturous" and "result-oriented."

The covered media device has to be physically damaged before the insured can demand software restoration cost, Selby said, but it never happened in EMOI's case. It is dangerous for courts to torture policy language and create ambiguity to find coverage, as Judge Tucker pointed out in the dissent, she added.

Policyholder attorneys, on the other hand, said the Ohio decision emboldens policyholders to fight for cyber coverage under traditional policies together with other recent court rulings favoring policyholders.

"The most interesting part of the ruling is this idea that ransomware can cause direct physical loss to software or data," said Emily Garrison, who represents policyholders at Honigman LLP. It "further demonstrates that cyber-related coverage for ransomware attacks can be found in traditional noncyber policies."

The ruling also shows "an example of the insurer's policy language not necessarily catching up with what's happening in the digital world," Garrison said. "The definition of media might have carried over from an older policy where it refers to film, magnetic and paper tapes."

In the EMOI suit, the policy defined media as material in which information is recorded, including "computer software and reproduction of data contained on covered media." The appeals panel found the fact that the policy identified "software" and "data '' to define media means that media is not just a physical device, so damage to EMOI's software, like the hacker's encryption, could be covered.

The panel's recognition that the policy does not only cover a media object, but also data stored on the device, is a recognition of how modern businesses operate, said Dan Healy of Anderson Kill PC.

"Most businesses are operating nearly entirely on electronic computerized networks," Healy said.

Businesses, especially small to midsize companies, **rely on property and liability insurance** for some kind of computer system and data restoration coverage, "especially because cyberinsurance is a tightening market with the scourge of ransomware attacks," said Josh Gold, Healy's colleague at Anderson Kill.

Gold noted that the ruling signals to policyholders that they may have more success beyond trial courts in their disputes over insurance coverage and whether cyber risks are included.

"It's certainly easier to go to your cyberinsurance company and say, please pay for this ransomware claim. But we don't know what the market's going to look like in a year or two," Gold said. "We do know that there are a lot of property and business package policies that promise some level of protection for policyholders' computer systems."

Marc Voses, a Clyde & Co. partner who represents insurers, said the Ohio majority's take on the definition of media is a "reminder for insurance policy drafters that clear policy language is key to establishing the scope of coverage provided."

The policy language "is not as precise given the modern-day computer usage as it could be," said Jonathan Schwartz of Goldberg Segalla LLP, who also represents insurers. "I do think that courts tend to struggle with sophisticated technology questions and how to fit a cyber event under a brick-and-mortar-type insurance policy that covers more traditional risks."

Schwartz said insurers should look for ways to clarify and tighten policy language to avoid rulings like the Ohio appellate court's.

Jack Kudale, CEO of cyberinsurer Cowbell, said traditional insurers' failure to catch up with their policyholders' digital development has caused them to suffer cyber losses. So the risks they scanned for before issuing the policy no longer matched the current risks faced by policyholders, he said.

"Their books have really grown to be so disconnected from the risk that they have underwritten," Kudale said, adding that insurers' rising cyber loss portfolios have also contributed to rate increases.

Lynda Bennett, chair of the insurance recovery practice at Lowenstein Sandler LLP, said hackers are constantly changing tactics in a way that challenges insurance policy language and forces constant adaptation by insurers and policyholders.

"When the policy language gets modified, the hackers are still two steps ahead and on to a different type of scam that doesn't fit neatly within the policy language," she said.

Instead of being optimistic like other policyholder attorneys, Bennett said she is concerned that the Ohio ruling is going to take the insurance industry one step closer to putting an absolute cyber exclusion in traditional policies. Bennett said she has seen insurers specifically exclude electronic data and information in property policies.

The Ohio ruling coupled with the ongoing wave of COVID-19 business-interruption coverage suits should lead policyholders to look at their policy renewal forms very carefully and see what changes insurers are making, she said.

"There's a lot of parallels here between what's going on in COVID-19 coverage fights," Bennett said. "The insurance companies take the position that physical loss is equivalent to damage to tangible property. But that's not what the language says."

That question of whether losing access to something is tangible damage, covered by a property policy, has recently doomed most of the hundreds of cases filed by businesses who claimed their insurers should have compensated them for revenue losses when the COVID-19 pandemic forced them to close.

Most courts have found that, even if the virus was present on a business' premises, it didn't represent a physical loss or damage to the property and therefore was not covered by insurance. Courts have also rejected policyholders' contentions that government-ordered closure orders represented a loss under their insurance contracts.

Schwartz, of Goldberg Segalla, said the Ohio majority interpreted "direct physical loss" in a way that ignores "virtually every" COVID-19 coverage ruling.

The Ohio majority's "suggestion that the policy needs to say the word 'tangible' in connection with physical damage is not really coming to grips with the existing body of [COVID-19] case law in Ohio and elsewhere," Schwartz said. "Courts have rejected the notion that there can be intangible loss of use."

Notably, the Ohio majority found EMOI does not need to show tangible physical damage to get coverage under its property policy because the insurance contract didn't include the term "tangible." The ruling echoes policyholder attorneys' favored argument that property damage does not require tangible harm and that loss of use of a property is covered.

But that decision conflates the concepts of loss of use with physical damage, so the case has a deficiency and does not have the precedential weight as policyholders may wish it had, said Josh Mooney, a Philadelphia-based partner with Kennedys CMK. The finding that EMOI's software could be physically damaged by the ransomware attack is illogical, he said.

"It's literally like saying if you put a lock on a door, you're physically damaging the doorway," Mooney said. "Ignoring the term 'physical damage' by leaving the world of tangible, the court, in essence, is changing the definition for direct physical damage into a loss of use."

--Additional reporting by Eli Flesch, Ben Zigterman and Shane Dilworth. Editing by Amy Rowe.
